



Код безопасности
ГК «Информзащита»

Встроенные или дополнительные сертифицированные средства защиты информации?

Зачем может понадобиться установка дополнительных средств защиты информации на общесистемное программное обеспечение при наличии сертифицированных встроенных средств защиты?

Термины

Встроенные СЗИ – сертифицированные СЗИ, встроенные в общесистемное программное обеспечение, обеспечивающие выполнение национальных требований к безопасности информации ограниченного доступа.

Дополнительные СЗИ – специальные сертифицированные продукты или пакеты безопасности, которые устанавливаются на общесистемное программное обеспечение в целях соответствия национальным требованиям к безопасности информации ограниченного доступа.

СЗИ – средства защиты информации.

Встроенные или дополнительные сертифицированные средства защиты информации?

Для чего могут понадобиться дополнительные СЗИ на общесистемное программное обеспечение при наличии встроенных сертифицированных СЗИ?

Проведение аттестации автоматизированной системы на базе встроенных сертифицированных СЗИ обладает рядом недостатков для клиентов:

- **Сложность обновления общесистемного программного обеспечения.**

Любое программное обеспечение имеет ошибки, которые нужно периодически исправлять. Любое программное обеспечение постоянно совершенствуется с целью улучшения его потребительских свойств. В результате исправлений исходного кода периодически выходят пакеты обновлений. **Обновления общесистемного программного обеспечения должны быть сертифицированы.** Если изменения незначительны, можно провести сертификацию только изменений по упрощенной процедуре – процедуре инспекционного контроля. Если изменения исходного кода превышают 10% всего кода, то необходимо проводить полную пересертификацию продукта. Сертификация операционной системы либо аналогичного по размеру исходного кода, общесистемного программного обеспечения занимает от полугода. Инспекционный контроль может быть проведен за пару месяцев.

Использование дополнительных СЗИ позволяет устанавливать все обновления на общесистемное программное обеспечение без риска потери аттестации и задержек на сертификацию обновлений общесистемного программного обеспечения.

- **Установка любого приложения, меняющего при установке системные (общие) бинарные модули общесистемного программного обеспечения, приводит к потере аттестации объекта информатизации.** Причины и решения те же, что и для обновлений.
- **Сертификация по Общим Уровням Доверия (ОУД)** – международная система сертификации, которая не получила в России широкого применения среди органов по аттестации и проектировщиков, поскольку в законодательстве и нормативных актах отсутствует четкое соответствие между тре-

бованиями по защищенности автоматизированных систем и уровнями доверия по ОУД. Наличие у СЗИ такого сертификата делает проект безопасности и аттестацию автоматизированной системы более дорогостоящими и рискованными.

Дополнительные СЗИ, сертифицированные по российским стандартам безопасности информации, позволяют снизить стоимость проекта безопасности и аттестации автоматизированной системы.

- **Сертификат на СЗИ от НСД, встроенные в общесистемное программное обеспечение, – это еще не все, что нужно для полноценного проекта безопасности и аттестации автоматизированной системы.** Необходимо выполнить требования к межсетевому экранированию, криптографии, защите от вторжений, антивирусной защите, централизованному управлению и мониторингу (для сетей ФСТЭК класса 1В и выше) и другим, согласно разработанному проекту безопасности. Поэтому необходимо рассматривать общую стоимость защиты и интеграцию этих СЗИ в части управления и мониторингу. Эксплуатация разнородных СЗИ – более рискованный (с точки зрения человеческих ошибок в эксплуатации) и дорогостоящий процесс.
- **По требованиям ФСТЭК к защите персональных данных (Приказ №58) СЗИ должны иметь сертификат НДВ 4.** Дополнительные СЗИ в подавляющем большинстве имеют сертификат не ниже НДВ 4. В то время как большинство встроенных СЗИ сертификата по НДВ не имеют вообще.
- **По требованиям ФСБ для защиты информации ограниченного доступа требуется применение сертифицированных СКЗИ (уровня, соответствующего модели угроз и нарушителя).** Распространенное общесистемное программное обеспечение не имеет такого сертификата на свои встроенные СКЗИ. Поэтому почти всегда следует применять дополнительные сертифицированные СКЗИ.
- **При работе в гетерогенных сетях (где используются одновременно Windows и Linux) разумно применять принцип унификации средств защиты. Как минимум в части средств управления и мониторинга событий ИБ.** В противном случае придется иметь два АРМ администратора ИБ и просматривать события ИБ в двух разных точках. Очевидно, что в этом случае также обосновано применение дополнительных СЗИ, позволяющих работать в гетерогенных сетях.

- **Централизованное управление, мониторинг событий ИБ и консолидация логов** обычно присутствует в дополнительных СЗИ от НСД, и отсутствует во встроенных. Обычно разработчик общесистемного ПО предлагает такие средства, но за дополнительную плату, так как такие средства представляют из себя отдельный коммерческий продукт.
- **Автоматическое продление сертификата по окончании его действия.** Производитель общесистемного ПО может не продлить сертификат на старую версию общесистемного ПО, так как срок действия сертификата (3-5 лет) версия общесистемного ПО может морально устареть и производитель уже продает новую версию. Производители Дополнительных СЗИ обычно автоматически продлевают сертификаты на свои средства пока ими пользуются клиенты, так как они сфокусированы именно на рынке сертифицированной ИБ, а не на рынке общесистемного ПО, кроме того, новые версии дополнительных СЗИ обычно поддерживают все распространенные версии общесистемного ПО, включая «морально устаревшие» (если, несмотря на это, они еще используются). Таким образом, клиенту не придется менять общесистемное ПО из-за того, что оно устарело и на него не продлили сертификат, если он использует дополнительное СЗИ.
- **Сертифицирована серия или производство?** Многие продукты со встроенными СЗИ сертифицированы только на серию, т.о. их может не быть в наличии в нужном количестве. Подавляющее большинство дополнительных СЗИ имеют сертифицированное производство.
- **Ограничение по применению сертифицированного СЗИ.** Большинство дополнительных СЗИ выпускается без существенных ограничений по применению. В то время как многие встроенные СЗИ выпускаются с существенными ограничениями по применению, в виду того, что данные средства разрабатывались без учета требований ФСТЭК/ФСБ, и отсутствующие функции должны деактуализироваться иными средствами или организационно-техническими мерами, что и указывается в ограничениях.



Код безопасности
ГК «Информзащита»

Тел.: +7 (495) 980-2345

E-mail: 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. «Код Безопасности» входит в группу компаний «Информзащита» – признанного лидера в сфере информационной безопасности – и является преемником её многолетних наработок в области создания средств защиты информации для государственных и коммерческих заказчиков.