Встроенные или дополнительные сертифицированные СЗИ?

В публикации раскрываются аспекты необходимости использования дополнительных средств защиты информации (СЗИ) на некоторое общесистемное ПО при наличии встроенных сертифицированных СЗИ.

Александр Ширманов – генеральный директор компании "Код Безопасности".

Введение

Инфраструктурное или общесистемное ПО, как правило, содержит встроенные СЗИ, обеспечивающие необходимый уровень безопасности для поддержания его бесперебойной работы, сохранности и целостности данных внутри системы. Согласно национальному законодательству страны, где такое ПО используется, в том числе и в России, эти СЗИ должны соответствовать требованиям безопасности, предъявляемым к автоматизированным системам, в которых обрабатывается информация ограниченного доступа. Как правило, это госучреждения и организации, где содержатся конфиденциальные сведения или гостайна. В России эти требования контролируются такими организациями, как ФСТЭК и ФСБ России. Система сертификации существует и у Министерства обороны. Во многих случаях как российские, так и зарубежные разработчики стремятся пройти сертификацию для того, чтобы быть уверенными в соответствии своих продуктов российскому законодательству и получить возможность аттестации автоматизированных систем с применением своего ПО в вышеупомянутых организациях.

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

Когда требуются дополнительные или встроенные СЗИ

Проведение аттестации автоматизированной системы на базе только встроенных сертифицированных СЗИ обладает рядом недостатков для клиентов. И тогда применяются дополнительные СЗИ – специальные сертифицированные продукты или пакеты безопасности, которые устанавливаются на общесистемное программное обеспечение. Среди недостатков можно отметить следующие.

1. Сложность обновления общесистемного программного обеспечения.

Любое программное обеспечение имеет ошибки, которые постоянно исправляются. 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 малы, 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.

2. 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.

3. Сертификация по Общим Уровням Доверия (ОУД).

Международная система сертификации ОУД не получила в России широкого применения среди органов по аттестации и проектировщиков, поскольку в законодательстве и нормативных актах отсутствует четкое соответствие между требованиями по защищенности автоматизированных систем и уровнями доверия по ОУД. Наличие у СЗИ такого сертификата делает проект безопасности и аттестацию автоматизированной системы более дорогими и рискованными. **Дополнительные СЗИ, сертифицированные по российским национальным стандартам безопасности информации, позволяют снизить стоимость проекта безопасности и аттестации автоматизированной системы.**

4. 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 интеграции этих СЗИ по управлению и мониторингу. Эксплуатация разнородных СЗИ – более рискованный (с точки зрения человеческих ошибок в эксплуатации) и дорогостоящий процесс.

5. 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 же время, большинство встроенных СЗИ сертификата на НДВ не имеют вообще.

6. По требованиям ФСБ для защиты информации ограниченного доступа необходимо 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.

7. 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 обоснованно применение дополнительных СЗИ, позволяющих работать в гетерогенных сетях.

8. Централизованное управление, мониторинг событий ИБ и консолидация логов обычно присутствуют в дополнительных СЗИ от НСД и отсутствуют во встроенных. Обычно разработчик общесистемного ПО предлагает такие средства, но за дополнительную плату, так как такие средства представляют собой отдельный коммерческий продукт.

9. 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.

10. Сертифицирована серия или производство?

Многие продукты со встроенными СЗИ сертифицированы только на серию, таким образом, их может не быть в наличии в нужном количестве. Подавляющее большинство дополнительных СЗИ имеют сертифицированное производство.

11. Ограничение по применению сертифицированного СЗИ.

Большинство дополнительных СЗИ выпускаются без существенных ограничений по применению. В то время как многие встроенные СЗИ выпускаются с существенными ограничениями по применению, ввиду 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.

Таким образом, применение дополнительных внешних СЗИ в проектах информационной безопасности автоматизированных систем становится решением большинства вышеперечисленных недостатков. Разработанные специально для обеспечения комплексной безопасности для аттестуемых автоматизированных систем дополнительные СЗИ обеспечат легитимность применения общесистемного ПО независимо от его происхождения и состояния его собственной сертификации. Чтобы выбрать подходящие дополнительные СЗИ, клиенту или интегратору следует обратить внимание не только на функциональные возможности, надежность и известность этих средств, но и на ряд организационных моментов, специфических для рынка информационной безопасности. Прежде всего, разработчик должен обеспечивать должную техническую поддержку и обновление сертификатов на свою продукцию. Здесь определенной гарантией является его известность на рынке, опыт работы и репутация. Наличие сети авторизованных партнеров – интеграторов, оказывающих услуги с применением дополнительных СЗИ – это второй важный фактор надежности. Наконец, клиенту следует обратить внимание и на доступность информации о СЗИ, которые он планирует применить, а также на наличие центров обучения для пользователей этих продуктов.

Александр Ширманов,
компания "Код Безопасности"