МСВСфера

ИНФЕРИТ

Чек-лист «Как выбрать сертифицированную ОС на российском рынке»

Кратко о важном

Не верьте пустым мифам!

Миф №1

«Если я приобрету сертифицированную ОС, то могу быть уверенным в ее безопасности»

Часто наличие сертификата соответствия не говорит о полной безопасности продукта. *Сертификат соответствия — это всего лишь свидетельство того, что обладающий им продукт соответствует тем или иным требованиям, предъявляемым регулятором в конкретной области.*

Например, сертифицированные ОС на рынке обычно соответствуют требованиям к ОС: согласно приказу № 119 ФСТЭК России, Профилю защиты операционных систем, а также Требованиям доверия согласно приказу № 76 ФСТЭК России. На сегодняшний день на российском рынке присутствуют ОС, которые не сертифицированы по требованиям безопасности информации, но при этом могут обеспечивать уровень безопасности не хуже, чем их сертифицированные конкуренты.

Поэтому выбирайте ОС исходя из задач вашей организации, чтобы она покрывала потребности и обеспечивала защиту данных!

Если информационная система вашей организации относится к ГИС, АСУ ТП, ИСПДн или является ЗОКИИ (требует соблюдения 17/21/31/239 приказов ФСТЭК, 152-ФЗ, 187-ФЗ), то в ней необходимо применять сертифицированную ОС.

Миф №2

«Большинство сертифицированных ОС отличаются набором средств защиты»

У сертифицированных ОС одного типа и класса защиты функции безопасности идентичны. Если вы не работаете с гостайной, нет смысла брать ОС выше 4 класса: дополнительные функции (мандатный доступ, маркировка) вам не понадобятся.

Миф №3

«Если я установлю последние обновления ОС, то на момент их установки я буду в полной безопасности»

На самом деле, это не так. На российском рынке превалирует 2 типа вендоров ОС: первые берут за основу операционные системы, которые создаются крупными мировыми проектами, такими как Debian или Red Hat, вторые же сами компонуют свою ОС из апстрима. В случаях, когда за основу взяты проекты Debian или RedHat, полученная в

результате ОС будет работать более стабильно и надежно, а компоненты таких систем будут более безопасны.

Проблема безопасности российских ОС заключается в том, что вендоры часто добавляют в ванильные версии дистрибутива (Debian, RHEL) не всегда тщательно проверенные пакеты или основывают системы на устаревших, неподдерживаемых версиях. Это создает риски из-за незакрытых уязвимостей.

Что же касается апстрима, то там другие риски: если вендор лишится обновлений от базового проекта и не будет иметь огромных ресурсов для решения задачи, то безопасность системы окажется под угрозой.

Выбор: Обращайте внимание **в первую очередь на частоту и содержание обновлений.** Обновления реже раза в полгода означают минимум год работы с уязвимостями. Идеально - раз в полгода или чаще. Также обращайте внимание на то, когда и какие уязвимости вендор устраняет в ОС.

Миф №4

«Если вендор заявляет о том, что у него реализован процесс по разработке безопасного ПО, значит все пакеты, входящие в ОС, проверяются в рамках различных видов тестирования и не содержат уязвимостей».

Современные ОС слишком сложны (миллионы строк кода, 1000+ пакетов), чтобы даже крупная команда исследователей могла полностью их проверить. Вендоры фокусируются на ключевых пакетах ("поверхности атаки", 30-50 штук), проверяя остальные лишь по базам известных уязвимостей и антивирусным сканерам.

Рекомендация: оцените уровень безопасности вендора так:

1. **Поищите публикации о ZeroDay уязвимостях** в его ОС на форумах и спецсайтах.. Если такую информацию получится найти — значит, в команде вендора работают квалифицированные исследователи безопасности программного обеспечения.
2. **Если публикаций нет, спросите вендора,** какой штат исследователей безопасности он содержит, и сколько ZeroDay-уязвимостей в год они находят?

   Маленькая команда (<10) или отсутствие ZeroDay — тревожный сигнал: вендор может не уделять безопасности должного внимания, фокусируясь только на прибыли.

Миф №5

«Если я приобрету техническую поддержку вендора, то это позволит мне очень быстро решать возникающие при работе с его ОС проблемы».

Недавно появившиеся на рынке вендоры часто экономят на технической поддержке из-за нехватки средств, что приводит к задержкам в решении проблем пользователей.

Рекомендация: тщательно проверьте качество *реальной* технической поддержки вендора до покупки:

1. **Протестируйте реакцию:** позвоните на "горячую линию" — дозвониться и получить ответ должно быть реально.
2. **Изучите отзывы:** поищите мнения пользователей о работе поддержки на форумах и порталах.

Миф №6

«Я приобрету сертифицированную ОС и вендор будет поддерживать данную систему в течении срока действия сертификата соответствия».

Вендоры на рынке чаще всего один раз получают сертификат соответствия на первую мажорную версию ОС и при выходе следующей версии он не получает новый сертификат, а обновляет уже существующий. При прекращении поддержки старой версии, вендор предлагает бесплатно новую, но **миграция между версиями Linux-дистрибутивов (основа российских ОС) крайне проблематична:**

- **Лучший случай:** потеря функциональности/данных в некоторых приложениях.
- **Худший:** требуется полная переустановка системы с потерей ВСЕХ данных и риском неработоспособности приложений.

Рекомендация: выбирайте ОС с **максимальным сроком поддержки мажорной версии** (выпуск обновлений) и **надежной, безболезненной процедурой миграции** на новые версии.

Узнать больше про российскую ОС «МСВСфера»

Чек-лист для подбора качественной и безопасной ОС

№	Вопрос	Ответ	Комментарий
1.	ОС имеет сертификат соответствия требованиям безопасности?		Если ответ «Нет», то прочитать статью «Безопасность корпоративных операционных систем: на что обращать внимание при выборе несертифицированной ОС на российском рынке» *(выйдет чуть позже, на месте этого текста появится ссылка)* и использовать чек-лист для выбора несертифицированных ОС
2.	Есть ли уникальные функциональные возможности (по сравнению с конкурентами), способствующие более защищенной работе в системе и (или) способствующие повышенному комфорту при использовании системы?		
3.	Минорные обновления ОС выходят не реже одного раза в 6 месяцев?		
4.	Минорные обновления ОС содержат информацию об устранении только новых уязвимостей (уязвимость, опубликованная в открытых источниках менее одного года назад)?		
4.1.	Старых уязвимостей менее 5% от числа устраненных в минорном обновлении?		Рассматривается, если ответ на вопрос № 4 отрицательный
5.	Критичность устраняемых в минорном обновлении ОС уязвимостей соответствует следующему распределению: 25% критических уязвимостей (CVSS > 7.0) на 75% некритических уязвимостей (CVSS < 7.0) ± 10%?		

6.	Вендор публикует в открытых источниках информацию об устраненных уязвимостях в ОС пакетом минорных или мажорных обновлений?		
7.	Есть ли в открытых источниках информация о проводимых исследованиях безопасности ОС и их результатах (обнаружение ZeroDay-уязвимостей, ошибок функционирвоания)?		
7.1.	Есть ли у вендора сотрудники, исследующие безопасность ОС (AppSec)?		Рассматривается, если ответ на вопрос № 7 отрицательный
7.2.	Штат исследователей (AppSec) больше 10 человек?		Рассматривается, если ответ на вопрос № 7 отрицательный
7.3.	Какое количество ZeroDay-уязвимостей и ошибок функционирования было найдено за предыдущий год?		Рассматривается, если ответ на вопрос № 7 отрицательный. Правильного ответа на этот вопрос нет. Чем больше будет число, тем лучше
8.	У вендора есть квалифицированная техническая поддержка, "реально" работающая 24/7/365?		
9.	Какой срок поддержки мажорной версии ОС (срок программных обновлений безопасности мажорной версии)?		Правильного ответа на этот вопрос нет. Чем больше будет число, тем лучше
10.	Есть ли возможность бесшовной миграции с предыдущей мажорной версии ОС на следующую без потери пользовательских данных и функциональности программ?		