

Александр Трубачев

Заместитель Председателя ООО «Центр безопасности информации» по НИР



Свободное программное обеспечение и доверие к безопасности информационных систем

Доверие к продукции

- **Функциональность**
- **Разработчик**
- **Где производится**
- **Независимые оценки**

Доверие к безопасности ИС

Доверие – основа для уверенности в том, что продукт или система ИТ отвечают установленным для них функциональным требованиям безопасности.

(Международный стандарт ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий»)

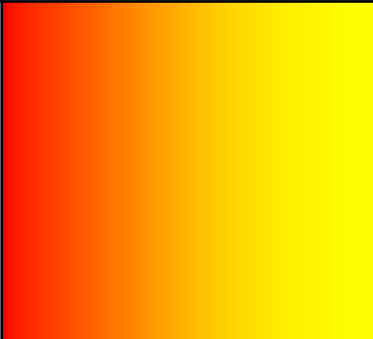
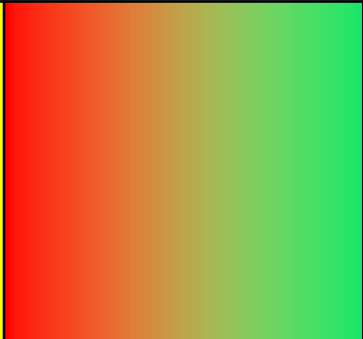
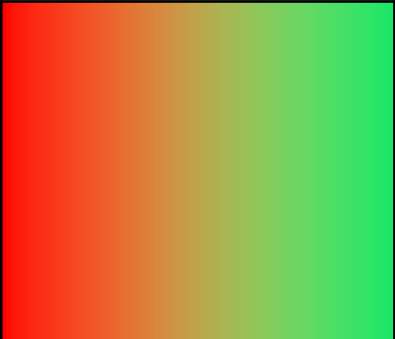
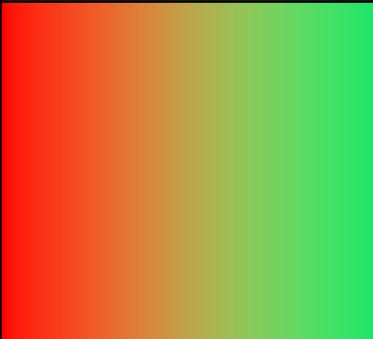
4 Требования доверия (assurance requirements)

- Качество проектных решений
 - Безопасность процесса разработки
 - Анализ уязвимостей
 - Поддержка
-
- Возможность сертификации

Виды программного обеспечения

- Открытое публичное ПО
- Открытое коммерческое ПО
- Проприетарное ПО с ограниченным доступом
- Закрытое проприетарное ПО

Качество проектных решений

Вид ПО	Открытое публичное ПО	Открытое коммерческое ПО	Проприетарное ПО с ограниченным доступом	Закрытое проприетарное ПО
Качество проектных решений				

Безопасность процесса разработки

Вид ПО	Открытое публичное ПО	Открытое коммерческое ПО	Проприетарное ПО с ограниченным доступом	Закрытое проприетарное ПО
Безопасность процесса разработки	[Red]	[Green]	[Green]	[Green]

Анализ уязвимостей

Вид ПО	Открытое публичное ПО	Открытое коммерческое ПО	Проприетарное ПО с ограниченным доступом	Закрытое проприетарное ПО
Анализ уязвимостей разработчиком	High	Medium	Medium	Medium
Анализ уязвимостей потребителем	Medium	Medium	Medium	High
Анализ уязвимостей специализированной организацией	Medium	Medium	High	High
Анализ уязвимостей злоумышленником	High	High	Medium	Medium




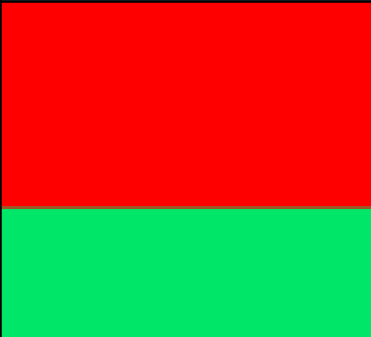
Безопасность процесса сборки

Вид ПО	Открытое публичное ПО	Открытое коммерческое ПО	Проприетарное ПО с ограниченным доступом	Закрытое проприетарное ПО
Доступность процесса сборки потребителю	High Risk (Red)	Medium Risk (Green)	Medium Risk (Green)	High Risk (Red)
Доступность процесса сборки специализированной организации	High Risk (Red)	Medium Risk (Green)	Medium Risk (Green)	High Risk (Red)

Поддержка

Вид ПО	Открытое публичное ПО	Открытое коммерческое ПО	Проприетарное ПО с ограниченным доступом	Закрытое проприетарное ПО
Поддержка	Red	Green	Green	Green

Возможность сертификации

Вид ПО	Открытое публичное ПО	Открытое коммерческое ПО	Проприетарное ПО с ограниченным доступом	Закрытое проприетарное ПО
Возможность сертификации				

Доверие к безопасности ПО

Вид ПО	Открытое публичное ПО	Открытое коммерческое ПО	Проприетарное ПО с ограниченным доступом	Закрытое проприетарное ПО
Качество проектных решений	Yellow	Green	Green	Green
Безопасность процесса разработки	Red	Green	Green	Green
Анализ уязвимостей разработчиком	Yellow	Green	Green	Green
Анализ уязвимостей потребителем	Green	Green	Green	Red
Анализ уязвимостей специализированной организацией	Green	Green	Yellow	Red
Анализ уязвимостей злоумышленником	Yellow	Yellow	Green	Green
Доступность процесса сборки потребителю	Orange	Green	Green	Red
Доступность процесса сборки специализированной организации	Orange	Green	Green	Red
Поддержка	Red	Green	Green	Green
Возможность сертификации	Orange	Green	Green	Red

Выводы

- 1. Открытое публичное ПО, с точки зрения доверия к безопасности, является не таким уж и привлекательным.**
- 2. Наибольшего доверия к безопасности можно достичь для открытого коммерческого ПО и проприетарного ПО с ограниченным доступом к коду и процессу сборки.**
- 3. Закрытое проприетарное ПО не может претендовать на высокие уровни доверия к его безопасности.**

14 Направления повышения доверия к безопасности ПО

1. Совершенствование нормативной базы

Для современных информационных технологий именно доверие является основным приложением усилий в направлении повышения их безопасности.

«При возрастании значимости безопасности для организаций и повышении восприимчивости информационных систем к расширенным долговременным угрозам нарушителей с высоким потенциалом не только имеют смысл, но требуются повышенные уровни доверия. ... Таким образом, когда потенциальное воздействие на деятельность и активы организаций, людей, другие организации и Nation является высоким, увеличивающийся уровень усилий должен быть направлен на обеспечение доверия.» NIST Special Publication 800-53

2. Повышение качества процессов разработки и поддержки ПО

3. Сертификация ПО

Специальные исследования доверия к безопасности ПО проводятся при сертификации на соответствие требованиям международного стандарта ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий» (Общие критерии) и при сертификации на отсутствие недекларированных возможностей.



Спасибо за внимание!

Трубачев Александр Павлович
Тел.: (495) 543-3060
mail: tap@cbi-info.ru