Александр Трубачев

Заместитель Председателя ООО «Центр безопасности информации» по НИР

Как обеспечить доверие к безопасности информационных систем

Безопасность информационных систем

Безопасность ИС определяется совокупностью организационных, технических, эксплуатационных и других мер и средств, которые применяются разработчиком, собственником и эксплуатирующей организацией для обеспечения требуемого уровня безопасности информации и ресурсов ИС в условиях действия различного рода угроз безопасности.

В современных взглядах на безопасность ИС принято выделять два основных аспекта безопасности, это **функциональность** и **доверие** к безопасности ИС

Функциональность безопасности

Функциональность безопасности ИС определяется теми функциями, механизмами и средствами их реализации, которые определены заказчиком в требованиях и предложены разработчиком в проектных решениях на создание ИС.

- Идентификация и аутентификация;
- Контроль доступа;
- Криптографическая защита;
- Защита взаимодействия;
- Аудит безопасности;
- Обеспечение целостности данных;
- Приватность:
- и др.

Функциональность безопасности ИС характеризуется количеством функций, мощностью и стойкостью механизмов, эффективностью средств обеспечения безопасности.

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»)

Доверенная информационная система - система, которая способна к действию в границах определенных уровней риска, несмотря на экологические разрушения, человеческие ошибки, структурные отказы и целеустремленные атаки, которые, могут иметь место в среде её эксплуатации.

Факторы, определяющие доверие к безопасности ИС

- Управление конфигурацией
- Поставка, установка, генерация и запуск
- Разработка, проектные решения
- Руководства пользователя и администратора
- Поддержка жизненного цикла, безопасность среды разработки, устранение недостатков
- Тестирование
- Оценка уязвимостей
- Поддержка доверия

Виды программного обеспечения

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

7 Возможности обеспечения доверия для различных видов ПО

Вид ПО	Открытое публичное ПО	Открытое отечественное коммерческое ПО	Открытое зарубежное коммерческое ПО	Проприетарное отечественное ПО с ограниченным доступом	Проприетарное зарубежное ПО с ограниченным доступом	Закрытое проприетарное ПО
РАЗРАБОТКА						
УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ						
ТЕСТИРОВАНИЕ						
ОЦЕНКА УЯЗВИМОСТЕЙ						
ПОДДЕРЖКА ЖИЗНЕННОГО ЦИКЛА						
РУКОВОДСТВА						
ПОСТАВКА И ЭКСПЛУАТАЦИЯ						
ПОДДЕРЖКА ДОВЕРИЯ						
ПРОИЗВОДСТВО						
ВОЗМОЖНОСТЬ СЕРТИФИКАЦИИ						

Общее количество уязвимостей различных продуктов ПО

	Вид ПО	Название продукта	Наименование поставщика	Общее число уязвимостей
ОС				
1	СО	Ядро Linux	Linux	**1155**
2	П	Mac Os X	Apple	**872**
3	П	Windows Xp	Microsoft	**726**
4	СК	Solaris	SUN	**533**
5	П	Windows 2000	Microsoft	**508**
6	П	Windows Vista	Microsoft	**461**
7	П	Windows Server 2008	Microsoft	**457**
8	П	Windows 2003 Server	Microsoft	**412**
9	П	Windows 7	Microsoft	**331**
10	П	AIX	IBM	**315**
11	СК	Enterprise Linux	Redhat	**253**
12	СК	Suse Linux	Suse	**208**
13	СК	Debian Linux	Debian	**192**
14	СК	Enterprise Linux Desktop	Redhat	**97**
Браузер				
1	СК	Firefox	Mozilla	**1051**
2	П	Safari	Apple	**464**
3	П	Internet Explorer	Microsoft	**264**

* По данным www.itsecdb.com

9 Среднее по годам применения количество уязвимостей различных продуктов ПО

	Вид ПО	Название продукта	Наименование поставщика	Общее число уязвимостей	Лет	Среднее в год
ОС						
1	СО	Ядро Linux	Linux	1155	16	**72**
2	П	Windows Server 2008	Microsoft	457	7	**65**
3	П	Windows 7	Microsoft	331	6	**55**
4	П	Mac Os X	Apple	872	16	**55**
5	П	Windows Xp	Microsoft	726	14	**52**
6	П	Windows Vista	Microsoft	461	9	**51**
7	СК	Solaris	SUN	533	12	**44**
8	П	Windows 2000	Microsoft	508	14	**36**
9	П	Windows 2003 Server	Microsoft	412	12	**34**
10	П	AIX	IBM	315	16	**20**
11	СК	Enterprise Linux	Redhat	253	13	**19**
12	СК	Suse Linux	Suse	208	12	**17**
13	СК	Debian Linux	Debian	192	16	**12**
14	СК	Enterprise Linux Desktop	Redhat	97	13	**7**
Браузеры						
1	СК	Firefox	Mozilla	1051	12	**88**
2	П	Safari	Apple	464	12	**39**
3	П	Internet Explorer	Microsoft	264	8	**33**

* По данным www.itsecdb.com

10 Средняя оценка опасности уязвимостей различных продуктов ПО

	Вид ПО	Название продукта	Наименование поставщика	Общее число уязвимостей	Число уязвимостей по уровням опасности									Средневзвешенная оценка
					0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+	
ОС															
1	П	Windows Vista	Microsoft	461		2	1		61	12	34	179	8	164	**8.2**
2	П	Windows Server 2008	Microsoft	457		1		2	61	16	34	178	6	159	**8.1**
3	П	Windows 2003 Server	Microsoft	412		1	11	2	21	46	29	174	3	125	**8.0**
4	П	Windows 7	Microsoft	331		1		1	50	7	21	153	1	97	**8.0**
5	П	Windows Xp	Microsoft	726		1	25	3	73	70	47	273	5	229	**7.9**
6	П	Windows 2000	Microsoft	508	1		26	5	43	91	28	174	2	138	**7.6**
7	П	AIX	IBM	315	2	5	19	3	33	25	26	151	1	50	**7.3**
8	СК	Suse Linux	Suse	208		2	29		21	36	13	78		29	**6.8**
9	П	Mac Os X	Apple	872	1	11	76	11	142	132	207	196	4	92	**6.6**
10	СК	Solaris	SUN	533		10	53	9	123	56	24	194		64	**6.6**
11	СК	Debian Linux	Debian	192		7	23	3	24	38	9	63	1	24	**6.6**
12	СК	Enterprise Linux Desktop	Redhat	97		_	18	2	15	18	8	22	1	13	**6.4**
13	СК	Enterprise Linux	Redhat	253		18	31	5	52	50	32	47	1	17	**5.9**
14	СО	Ядро Linux	Linux	1155	1	78	194	32	381	99	108	235	3	24	**5.4**
Браузеры															
1	П	Internet Explorer	Microsoft	264			2		24	7	6	6	2	217	**9.3**
2	П	Safari	Apple	464		3	13		108	64	37	37	3	199	**7.6**
3	СК	Firefox	Mozilla	1051		1	46	3	185	177	94	112	1	432	**7.6**

* По данным www.itsecdb.com

Базовые принципы безопасности ПО

- Простота
- Модульность
- Иерархическое представление
- Изоляция доменов
- Наименьшее количество полномочий
- Наименьшее количество функциональности
- Изоляция/инкапсуляция ресурсов

Выводы

1. Наибольшего доверия к безопасности ИС можно достичь при использовании **отечественного** открытого коммерческого ПО и проприетарного ПО с ограниченным доступом к коду и процессу сборки
2. Закрытое проприетарное ПО не может обеспечить высокие уровни доверия его безопасности ИС

Направления повышения доверия к безопасности ИС

1. Совершенствование нормативной базы, учет в ней требований доверия к безопасности ИС

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 Нацию 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 требования 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