Операционная система на компьютере: правовые и коммерческие риски

ВВЕДЕНИЕ

В последнее время участились случаи хищения информации, содержащей коммерческую тайну, в том числе, посредством использования компьютерных сетей.

Аналитический центр Zecurion Analytics представил результаты ежегодного исследования об утечках конфиденциальной информации в мире и в России за 2012 год. Самыми показательными и громкими российскими утечками аналитики называют ситуации в МВД, Следственном комитете, концерне «Тракторные заводы». Также «разглашаемостью» данных отличаются мобильные операторы и сайты-купонаторы.

Общий ущерб от утечек конфиденциальной информации в 2012 году остался примерно на уровне прошлого года (20,582 млрд доллл.) и составил $20,083 млрд. Число российских утечек с ощутимым потенциальным ущербом осталось примерно на уровне прошлого года (36 в 2012 году против 41 в 2011 году), что составило 4% мировых сливов информации. При этом доля утечек из США (69% от общего числа) продолжает постепенно снижаться, несмотря на постоянно возникающие в СМИ крупные скандалы. Также существенные доли имеют Великобритания, Канада, Австралия, Индия.

Поменялся и отраслевой профиль утечек. Если в 2011 году больше всего утечек было зарегистрировано в отрасли здравоохранения, то по итогам 2012 года медучреждения оказались только четвёртыми после учебных заведений (20,1%), госорганизаций (16,9%) и предприятий розничной и интернет-торговли (12,4%). Сведения об утечках других типов информации (коммерческой тайны, интеллектуальной собственности и пр.) встречаются реже. Периодически СМИ сообщают даже о случаях раскрытия гостайны, обнаружении документов с грифами секретности. Но далеко не всегда можно оценить ущерб таких утечек и понять, представляет ли подобная информация ценность. Наиболее распространённые каналы утечек — это веб-сервисы (20,5%), ноутбуки и планшеты (16,5%), а также мобильные телефоны (11,1%). Большая доля утечек по-прежнему происходит случайно, из-за ошибок или халатности собственных сотрудников.

Планируемое в 2013 году ужесточение штрафных санкций за разглашение персональных данных в России и Евросоюзе приведёт к серьёзному увеличению финансового ущерба от утечек. Готовиться к повышению штрафных санкций стоит не только компаниям, работающим на европейских рынках, но и сугубо российским фирмам. Доработки законодательства в части защиты персональных данных идут в России полным ходом, и уже в феврале 2013 года член Совета Федерации и председатель комиссии по развитию информационного общества Руслан Гаттаров сообщил, что штрафы за утечки персональных данных для юридических лиц должны исчисляться миллионами рублей.

http://rbcdaily.ru/society/562949987433402

Все мы хотим, что бы используемое нами программное обеспечение было не только удобным, но надёжным в части защиты конфиденциальной информации.

Для начала попробуем ответить, какими критериями можно руководствоваться при решении вопроса надёжности программного обеспечения в этой области.

Кто-то выбирает программное обеспечение, ориентируясь на количество потраченных на его разработку финансовых ресурсов, кто-то ориентируется на авторитетное имя в названии[1], а кто-то руководствуется своим личным опытом.

Критериев отбора может быть великое множество, и многие из них на самом деле, являются лишь субъективным выбором, сформированным, в том числе и на основании удачной маркетинговой политики.

Я ничуть не настаиваю на том, что определение надёжности программного обеспечения может определяться только каким-то, мне понравившимся способом. Но всё же обращу внимание читателя на ряд нормативных документов, которыми

1 Пример - Kaspersky Total Security

государство регулирует этот вопрос.

Речь идёт о государственной сертификации программного обеспечения на предмет наличия недекларированных возможностей (программных закладок), а также качества реализации систем защиты от несанкционированного доступа.

Наиболее серьёзно к данному вопросу подошли военные — Минобороны РФ разработало свою операционную систему — МС ВС, которая прошла наиболее полную государственную сертификацию, что позволило получить гарантию защиты данных от третьих лиц и предотвратить их утечку.

Однако что есть в распоряжении коммерческих компаний либо государственных предприятий за пределами военно-промышленного комплекса?

Особенно остро этот вопрос возник в процессе развития действующего законодательства о защите персональных данных и в связи с резко возросшим количеством краж информации, содержащей коммерческую тайну.

Кроме того, недавние разоблачения Эдварда Сноудена, касающиеся деятельности АНБ США, существенно обострили проблему защиты информации.

Как следует из материалов Сноудена, США (прежде всего, американским спецслужбам) удалось еще в 2000 году пролоббировать в качестве международного стандарта шифрования алгоритм AES, который имеет уязвимости в математическом аппарате. Наличие подобных «закладок» позволяет американским спецслужбам практически на лету дешифровать сообщения, защищенные любой системой, использующей данный алгоритм шифрования. А он является одним из самых распространенных.

Из документов Сноудена следует, что спецслужбы США порой договариваются с лояльными компаниями-разработчиками средств защиты. АНБ делает специальные вставки (backdoor) в средства шифрования (оборудование и программы), позволяющие ей легко обходить разрабатываемые этими компаниями криптографические механизмы. Иногда АНБ приходится за это платить: на подобные цели агентство ежегодно тратит около $250 млн. в рамках секретной программы Bullrun.

http://www.kommersant.ru/pda/news.html?id=2272491

Безусловно, такие сведения не могли не повлечь за собой соответствующую реакцию контролирующих органов.

Интересующиеся могут пройти на сайт Генеральной прокуратуры РФ и посмотреть сводный план проверок на 2014 г.

Согласно данному плану запланированы **множественные проверки** хозяйствующих субъектов со стороны Федеральной службой по техническому и экспортному контролю (далее - ФСТЭК).

Так, например по запросу «ФСТЭК» на предмет проверяемых в 2014 г. организаций, интернет-сайт Генпрокуратуры РФ[2] выдаёт следующее: **«По Вашему запросу найдено слишком большое количество плановых проверок. Попробуйте уточнить поисковый запрос, сократив период проверки»**.

Полномочия ФСТЭК определены Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085:

1) обеспечения безопасности (некриптографическими методами[3]) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том

2 http://plan.genproc.gov.ru

3 Для понимания читателей, замечу, что обеспечение защиты криптографическими методами входит в компетенцию другой службы, а именно, Федеральной службы безопасности РФ.

числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;

2) противодействия иностранным техническим разведкам на территории Российской Федерации;

3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;

4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

Учитывая указанные специфические полномочия ФСТЭК, нетрудно понять что скрывается за общими словами цели всех проверок: «предупреждение, выявление и пресечение нарушений лицензионных условий и требований».

Грубо говоря, можно назвать 2014 г. - годом проверок соблюдения требований нормативных документов, касающихся защиты информации.

Для понимания сути вопроса мною взяты для сравнения 2 наиболее распространённых объекта сертификации ФСТЭК и ФСБ РФ операционные системы: Windows и Linux. Популярная операционная система iOS, используемая в продуктах компании Apple в обзор не включена по причине полного отсутствия сертификатов.

Linux — общее название Unix-подобных операционных систем, основанных на одноимённом ядре. Ядро Linux создаётся и распространяется в соответствии с моделью разработки свободного и открытого программного обеспечения. Поэтому общее название не подразумевает какой-либо единой «официальной» комплектации Linux; они распространяются в основном бесплатно в виде различных готовых дистрибутивов, имеющих свой набор прикладных программ и уже настроенных под конкретные нужды пользователя.

Дистрибутив Linux — общее определение операционных систем, использующих ядро Linux, готовых для конечной установки на пользовательское оборудование. Кроме ядра и, собственно, операционной системы, дистрибутивы обычно содержат широкий набор приложений, таких как редакторы документов и таблиц, мультимедиа-проигрыватели, системы для работы с базами данных, и т. д.

В настоящее время существует более шестисот дистрибутивов Linux; более половины из них поддерживаются в актуальном состоянии, что обеспечивается регулярным выпуском обновлений разработчиками дистрибутива[4].

https://ru.wikipedia.org

Сведения о фактической сертификации получены из Государственного реестра сертифицированных средств защиты информации № РОСС RU.0001.01БИ00[5] ФСТЭК и Перечня средств защиты информации, сертифицированных ФСБ России[6].

Каждый из читателей, кому приходится сталкиваться по роду деятельности с информацией, составляющей государственную тайну, сможет сопоставить используемое им программное обеспечение и оценить соблюдение требований нормативных актов по обеспечению её защиты.

4 По некоторым оценкам, известно более 2000 дистрибутивов Linux
5 http://fstec.ru/component/attachments/download/489
6 http://clsz.fsb.ru/certification.htm

1. Сертификация ФСТЭК

ФСТЭК сертифицирует операционные системы, а также межсетевые экраны, антивирусное программное обеспечение а также программно-аппаратные комплексы, предназначенные для защиты информации либо доля разграничения доступа к ней.

Как уже было сказано выше, ограничимся исключительно требованиям к операционным системам.

1.1 Классификация по уровню контроля отсутствия недекларированных возможностей

Данная классификация осуществляется в соответствии с требованиями Руководящего документ а «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации . Классификация по уровню контроля отсутствия недекларированных возможностей », утвержденного решением председателя Государственной технической комиссии при Президенте Российской Федерации от 04.06.1999 г. № 114

Самый высокий уровень контроля - первый, достаточен для ПО, используемого при защите информации с грифом «ОВ».

Второй уровень контроля достаточен для ПО, используемого при защите информации с грифом «СС».

Третий уровень контроля достаточен для ПО, используемого при защите информации с грифом «С».

Самый низкий уровень контроля - четвертый, достаточен для ПО, используемого при защите конфиденциальной информации.

Тип	Объект сертификации	Уровень контроля			
		4	3	2	1
	Все версии Windows (XP, 7, 8, Server и т.д.)[7]				
	Red Hat Enterprise Linux 4[8]				
	ALT Linux 4.0 SE				
	Trustverse Linux XP Desktop 2008 SE				
	SUSE Linux Enterprise Server 11 SP 1				
	Mandriva Linux 2010.2 Powerpack				
	МСВСфера Server 5.2				

7 Не сертифицированы по данному критерию
8 Здесь и далее указано название дистрибутива Linux

Тип	Объект сертификации	Уровень контроля
	Альт Линукс СПТ 6.0	
	МСВС 3.0[9]	
	Astra Linux Special Edition	
	ROSA Linux 2011	
	«Циркон 26К» (на базе Debian GNU/Linux)	
	Янукс 3.0	

Таблица 1: Классификация по уровню контроля отсутствия недекларированных возможностей

Читатель наверняка отметил, что ни одна из версий операционной системы Windows не прошла сертификацию по данному критерию.

ОАО "Северное Проектно-Конструкторское Бюро" анонсировало разработанную ими защищенную облачную платформу "Глобула" на основе Astra Linux Special Edition и открытого проекта OpenStack. «Глобула» предназначена для построения закрытых защищенных вычислительных облаков, соответствующих требованиям ФСТЭК для систем класса АС.

«Глобула» может быть использована для построения инфраструктуры обеспечения доступа к выделенным вычислительным ресурсам (сети, сервера, сервисы и приложения).

Облачная платформа «Глобула» совместно с ОС «Astra Linux Special Edition» образует систему, удовлетворяющую следующим требованиям ФСТЭК России: уровень контроля отсутствия НДВ 2; класс защищенности от НСД к информации 1Б. Это решение может применяться в составе автоматизированных систем, обрабатывающих информацию ограниченного распространения, включая сведения с грифом «совершенно секретно».

http://uinc.ru/news/sn19175.html

1.2 Классификация по показателям защищенности от несанкционированного доступа к информации.

Данная классификация определяется на основании Руководящего документ а «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утвержденного решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992 г.

9 Мобильная система вооружённых сил Российской Федерации, основана на Linux, по ряду источников сообщается о фактическом уровне контроля 1 НДВ

	Объект сертификации	Класс защищённости					
		6	5	4	3	2	1
	ОС МСВС 3.0						
	ALT Linux 4.0 Desktop Professional						
	Mandriva Corporate Server 4 Update 3						
	Mandriva PowerPack 2008						
	Trustverse Linux XP Desktop 2008 Secure Edition						
	Альт Линукс СПТ 6.0						
	Astra Linux Special Edition						
	ROSA Linux 2011						
	«Циркон 26К» (на базе Debian GNU/Linux)						
	CentOS релиз 6.2						
	SUSE Linux Enterprise Server 11 SP 1						
	«Mandriva Linux 2010.2 Powerpack»						
	Microsoft Windows Server 2012[10]						
	«Microsoft Windows 8», «Microsoft Windows 8 Профессиональная», «Microsoft Windows 8 Корпоративная»[11]						
	MS Windows Server 2008 Standard Edition						
	Microsoft Windows Server 2008 Enterprise Edition						
	Microsoft Windows Server 2008 Datacenter						
	Операционная система Microsoft Windows 7 в редакциях «Профессиональная», «Корпоративная» и «Максимальная»[12]						
	Операционная система Microsoft Windows 7 (SP1) в редакциях «Профессиональная», «Корпоративная» и «Максимальная»						

Таблица 2: Показатели защищённости

10 При условии соблюдения ограничений в виде соблюдения процедуры контроля соответствия (верификации) сертифицированному эталону, установки всех актуальных сертифицированных обновлений безопасности настройки и контроля механизмов защиты безопасности в соответствии с «Руководством по настройке системы»

11 При условии установки всех актуальных обязательных сертифицированных обновлений безопасности и выполнения указаний по эксплуатации, приведенных в формулярах 501110-001-82487552-2013 01 ФО и 501110-001-82487552-2013 02 ФО

12 При условии соблюдения ограничений в виде соблюдения процедуры контроля соответствия (верификации) сертифицированному эталону, установки всех актуальных сертифицированных обновлений безопасности настройки и контроля механизмов защиты безопасности в соответствии с «Руководством по настройке системы»

Операционная система Astra Linux Special Edition (разработка ОАО «НПО РусБИТех») успешно прошла тематические исследования в системе сертификации средств защиты информации ФСБ России. В ходе проведенных исследований подтверждено соответствие операционной системы требованиям безопасности информации, содержащей сведения, составляющие государственную тайну.

На сегодняшний момент система Astra Linux Special Edition является **единственной в России операционной системой**, прошедшей сертификацию во всех обязательных системах сертификации средств защиты информации (Минобороны России, ФСБ России, ФСТЭК России) и в которой можно обрабатывать информацию ограниченного доступа, включая сведения, составляющие государственную тайну до степени секретности «совершенно секретно» включительно.

http://www.npo-echelon.ru/news/10294/?sphrase_id=58388

1.3 Класс защиты от несанкционированного доступа для многопользовательских автоматизированных систем

Класс защиты определяется в соответствии с Руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденного решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992 г.

Автоматизированные группы подразделяются на 3 класса защиты.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

	Объект сертификации	1Д	1Г	1В	1Б	1А
	Microsoft Windows 2003 Server Standard Edition					
	Microsoft Windows 2003 Server Enterprise Edition Release 2					
	Microsoft Windows 2003 Server Standard Edition (SP2)					
	Microsoft Windows 2003 Server Standard Edition Release 2 с пакетом обновлений Service Pack 2					

	Объект сертификации	1Д	1Г	1В	1Б	1А
	Microsoft Windows XP Professional SP2					
	Microsoft Windows Vista (SP1)					
	Microsoft Windows Server 2008 Standard Edition					
	Microsoft Windows Server 2008 Enterprise Edition					
	Microsoft Windows 7 в редакциях «Профессиональная», «Корпоративная» и «Максимальная»					
	Microsoft Windows Server 2008 R2 в редакциях Standard, Enterprise и Datacenter					
	Microsoft Windows 7 (SP1) OEM в редакции «Профессиональная»					
	Microsoft Windows 7 Service Pack 1 **with Secure Pack Rus 3.0**,					
	Trustverse Linux XP Desktop 2008 Secure Edition					
	МСВСфера 5.2 Desktop/Server					
	Novell SUSE Linux Enterprise Server 10					
	ОС МСВС 3.0					
	Astra Linux Special Edition					
	Alt Linux СПТ 6.0					
	Oracle Enterprise Linux 5 Update 2 в редакции x86_64					
	ROSA Linux 2011					
	SUSE Linux EnterpriseServer 11 ServicePack 1					
	Янукс 3.0					

Таблица 3: Класс защищённости для многопользовательских систем

Такой высокий класс защищённости ряда дистрибутивов Linux стал возможен за счет реализации разработчиками отечественной версии «мандатного управления доступом».

Согласно требованиям ФСТЭК, мандатное управление доступом или «метки доступа» являются ключевым отличием систем защиты государственной тайны РФ старших классов 1В и 1Б от младших классов защитных систем на классическом разделении прав по матрице доступа.

В таких системах, например запрещено копирование данных из секретного документа в документ с более низкой степенью секретности.

BG: А чем занимается Secure Pack Rus?

директор по информационной безопасности компании Microsoft Владимир Мамыкин: Так

как это не наша разработка, то мы не старались особо вникать ее суть. Просто без нее получить сертификат ФСБ было нельзя — **что-то там в нашей системе не удовлетворяло их требованиям**. А с этим модулем все требования ФСБ выполняются. Вообще говоря, во многих странах есть свои требования к системам, используемым в госструктурах. И не всегда эти требования доступны. Это есть и в Европе, и в Японии, и в США. Это нормально.

http://www.kommersant.ru/doc/759779

Средство защиты информации Secure Pack Rus версия 3.0 (СЗИ SPR 3.0) является сервисным пакетом для операционных систем семейства Microsoft Windows и позволяет обеспечить выполнение требований ФСБ России по защите конфиденциальной информации по классу АК2 и АК3 для обработки информации ограниченного распространения (конфиденциальная информация, персональные данные), **не содержащей сведений, составляющих государственную тайну**.

http://www.cansec.ru/products/21.html

1.4 Оценочный уровень доверия

Оценочный уровень доверия (далее - ОУД) определяется в соответствии с приказом председателя Гостехкомиссии России от 19 июня 2002 года № 187.

ОУД1 применим, когда требуется некоторая уверенность в правильном функционировании, а угрозы безопасности не рассматривают как серьезные.

ОУД2 применим в случаях, когда разработчикам или пользователям требуется независимо подтверждаемый уровень доверия от невысокого до умеренного при отсутствии доступа к полной документации по разработке.

ОУД3 применим в тех случаях, когда разработчикам или пользователям требуется независимо подтверждаемый умеренный уровень доверия на основе всестороннего исследования ОО и процесса его разработки без существенных затрат на изменение технологии проектирования.

ОУД4 – самый высокий уровень, на который, вероятно, экономически целесообразно ориентироваться при оценке уже существующих продуктов.

Поэтому ОУД4 применим, когда разработчикам или пользователям требуется независимо подтверждаемый уровень доверия от умеренного до высокого в ОО общего назначения и имеется готовность нести дополнительные, связанные с обеспечением безопасности, производственные затраты.

	Объект сертификации	Оценочный уровень доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
	Янукс 3.0							
	Red Hat Enterprise Linux AS, WS Version 4 Update 1+Audit Pack							
	МСВСфера 5.2 Desktop/Server							

	Объект сертификации	Оценочный уровень доверия
	ОС Microsoft Windows Server 2008 Standard/Enterprise Edition	
	Microsoft Windows XP Professional	
	Microsoft Windows Vista (SP1)	

Таблица 4: Оценочный уровень доверия

2. Сертификация ФСБ РФ

Непосредственная деятельность по сертификация ФСБ РФ регламентирована ФЗ «О государственной тайне», постановлением Правительства Российской Федерации от 26.06.95 г. № 608 «О сертификации средств защиты информации» и приказом ФСБ РФ от 13 ноября 1999 г. № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия».

Согласно ст. 28 ФЗ «О государственной тайне», средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

В соответствии с п. 1.4 Приказа ФСБ РФ № 564, органы по сертификации системы сертификации проводят обязательную сертификацию средств защиты информации, используемых при работе со сведениями, составляющими государственную тайну, в том числе иностранного производства.

При этом по правилам системы сертификации по инициативе разработчика, изготовителя или потребителя может также проводиться добровольная сертификация средств защиты информации, не предназначенных для работы со сведениями, составляющими государственную тайну.

	Объект сертификации	**Возможность обработки информации, содержащей гостайну**
	«Операционная система Microsoft Windows Server 2003 R2 Service Pack 2 со встроенными и дополнительно интегрируемыми механизмами обеспечения безопасности, реализуемыми средством защиты информации «Secure Pack Rus версия 3.0 (исполнения 1, 2)»»	может использоваться для защиты информации, **не содержащей** сведений, составляющих государственную тайну
	«Операционная система Microsoft Windows 7 Ultimate Service Pack 1 со встроенными и дополнительно интегрируемыми механизмами обеспечения безопасности, реализуемыми средством защиты информации «Secure Pack Rus версия 3.0 (исполнения 1, 2)»»	может использоваться для защиты информации, **не содержащей** сведений, составляющих государственную тайну
	«Операционная система Microsoft Windows Server 2008 R2 Standard (или Enterprise) Service Pack 1 со встроенными и дополнительно интегрируемыми механизмами обеспечения безопасности, реализуемыми средством защиты информации «Secure Pack Rus версия 3.0 (исполнения 1, 2)»»	может использоваться для защиты информации, **не содержащей** сведений, составляющих государственную тайну
	Astra Linux Special Edition	может использоваться для обработки информации, **содержащей** сведения, составляющие государственную тайну

Таблица 5: Сертификация Федеральной службой безопасности

Средство контроля защищенности защищенности информационных систем «Сканер-ВС» (разработка НПО «Эшелон») успешно прошла тестирование на совместимость с национальной защищенной операционной системой **Astra Linux Special Edition**.

«Сканер-ВС» предназначен для комплексного тестирования защищенности информационных систем. Особо подчеркнем слово «комплексный», т.к. продукт заключает в себе множество самых разнообразных модулей: поиск и проверка уязвимостей, перехват и анализ сетевого трафика, контроль целостности, аудит Wi-Fi сетей и др. Использование «Сканер-ВС» позволяет обеспечить соответствие организации требованиям многочисленных нормативных документов, таких как Постановление Правительства РФ 2007 г. N 781, приказ ФСТЭК России 2010 г. N 58, руководящие документы Гостехкомиссии.

Сочетание Astra Linux Special Edition и «Сканер-ВС» повышает уровень защищенности информационной системы, позволяя оперативно контролировать появление уязвимостей в сетевых сервисах и настройках системы. Напомним, что сертифицированная в Минобороны России Astra Linux Special Edition недавно прошла сертификацию и во ФСТЭК России, тем самым открыв свои возможности не только силовым ведомствам и государственным учреждениям, но и коммерческим организациям (например, теперь данную ОС можно использовать для защиты персональных данных). «Сканер-ВС» так же обладает сертификатами обоих ведомств, что выгодно выделяет продукт среди аналогичных (хотя полных аналогов продукта не существует).

«Astra Linux Special Edition – это, безусловно, инновационная операционная система, которая подтвердила свой статус, став национальной защищенной операционной системы страны. Компания «Эшелон» рада возможности внести свою лепту в её развитие, так модули Сканер-ВС для локального и сетевого аудита стойкости паролей вошли в стандартную поставку операционной системы», - комментирует генеральный директор ЗАО «НПО «Эшелон» Алексей Марков.

http://b2blogger.com/pressroom/128505.html

Специалистами компаний Актив и НПО «РусБиТех» проведено совместное тестирование, которое выявило совместимость электронных идентификаторов Рутокен ЭЦП и Рутокен S и сертифицированной операционной системы **Astra Linux Special Edition**.

ОС Astra Linux сертифицирована во ФСТЭК по 3 классу защищенности СВТ и 2 уровню контроля отсутствия недекларированных возможностей. Рутокен S сертифицирован во ФСТЭК по 3 уровню контроля отсутствия недекларированных возможностей, а Рутокен ЭЦП по 4 уровню отсутствия недекларированных возможностей.

Решение может применяться в информационных систем, обрабатывающих конфиденциальную информацию и персональные данные, вплоть до информации с грифом «С». Его использование позволяет обеспечить соответствие информационных систем нормам российского законодательства и требованиям регуляторов.

http://www.aktiv-company.ru/news/rutoken-news-26-06-2012.html

3. Сертификация Минобороны РФ

В системе сертификации Министерства обороны РФ в перечень средств защиты информации Минобороны РФ попадают все технические изделия в защищенном исполнении, информационные системы, защищенное программное обеспечение, программные средства общего назначения, программные средства обработки информации в АСУ, парольные системы, ТСЗИ, в том числе уничтожители, и др.

Создание системы сертификации в Минобороны России предусмотрено Постановлением Правительства РФ от 26.06.1995 года № 608 «О сертификации средств защиты информации».

В Министерстве обороны РФ требования по сертификации определены Приказом МО РФ от 28.01.1998 г. № 54 и приказом № 058 от 1996 г., которым определён перечень средств защиты информации, подлежащих сертификации в системе сертификации Минобороны России по требованиям безопасности информации.

Также при сертификации для нужд Минобороны необходимо руководствоваться национальными стандартами РФ, в том числе:

- ГОСТ Р 51189 «Средства программные систем вооружения. Порядок разработки»,
- ГОСТ Р 51583-2000 «Порядок создания автоматизированных систем в защищенном исполнении», согласно которому научно-техническое обеспечение создания автоматизированных средств защиты информации должно соответствовать современному состоянию развития науки и техники. Выпускаемые средства должны иметь сертификаты соответствия, полученные в соответствующих системах сертификации по требованиям безопасности информации.

Деятельность в области создания (проектирование, разработка, реализация, испытания, сопровождение и др.) средств защиты информации в Минобороны России подлежит обязательному лицензированию. В МО РФ выдается только одна лицензия - это лицензия МО РФ[13].

В настоящее время на сайте Минобороны РФ доступен[14] **проект** приказа Министра обороны Российской Федерации «Об утверждении Административного регламента предоставления Министерством обороны Российской Федерации государственной услуги по лицензированию деятельности органов военного управления, соединений, воинских частей и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны».

Согласно этому **проекту**, будет признан утратившим силу приказ Министра обороны Российской Федерации от 28 января 1998 г. № 54 «О создании в Министерстве обороны Российской Федерации системы лицензирования деятельности органов военного управления, объединений, соединений, воинских частей, учреждений, военно-учебных заведений, предприятий и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, а также с созданием средств защиты информации, относящихся к его компетенции».

При этом, согласно **проекту**, контроль за указанной деятельностью будет возложен на Восьмое управление Генерального штаба Вооруженных Сил Российской Федерации .

В настоящее время, из двух операционных систем (Windows и Linux), в системе Минобороны сертифицированы только операционные системы на базе Linux: МСВС 3.0,

13 http://www.npo-echelon.ru/news/1158/
14 http://stat.doc.mil.ru/documents/projects/more.htm?id=11487888@morfNPAProject

МСВС 5.0 и Astra Linux Special Edition.

Среди защищенных решений, разрабатываемых компанией НПО «Эшелон», есть уникальные продукты, совместимые с Astra Linux Special Edition, например: комплекс контроля эффективности системы защиты информации, тестирования и анализа защищенности «СКАНЕР-ВС» и комплекс межсетевого экранирования и обнаружения вторжений «РУБИКОН».

Принципиально важно, что комплекс «РУБИКОН» на текущий момент является единственным межсетевым экраном, поддерживающим так называемые мандатные метки, использование которых позволяет легитимно организовать разграничение информационных потоков на сетевом уровне в соответствии с грифом обрабатываемой информации (в системах, построенных на базе ОС Astra Linux Special Edition)/

http://www.infosecurityrussia.ru/news/9488

Работы по созданию государственной автоматизированной системы "Гособоронзаказ" (ГАС "ГОЗ") близятся к завершению.

Как рассказал "Известиям" Владимир Минаев, гендиректор ОАО "Системы управления", выигравшего тендер на разработку системы, ГАС "ГОЗ" будет работать на российских спецкомпьютерах "Эльбрус" с отечественной операционной системой Astra Linux Special Edition, сертифицированной для работы с документами с грифом "совершенно секретно". Между собой машины соединят закрытой линией связи, похожей на правительственную связь АТС-1 и АТС-2.

— Первоначально абонентами системы станут чиновники более 40 министерств и ведомств, участвующих в формировании и исполнении ГОЗа. В перспективе к системе подключат руководителей более 5 тыс. оборонных предприятий, — рассказал Минаев.

http://izvestia.ru/news/518788#ixzz1paDUivWd

4. Информационные системы персональных данных

Ещё один вид информации, подлежащий защите — это персональные данные. В соответствии со ст. 7 ФЗ «О персональных данных», операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

При этом, в соответствии с п. 3 ст. 18.1 указанного закона, оператор обязан принимать необходимые и достаточные организационные и технические меры по обеспечению безопасности персональных данных.

Согласно ст. 19 этого же закона, оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

При этом Правительство российской Федерации устанавливает уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных.

Такие уровни установлены «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утверждёнными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 .

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Чтобы отнести типовую информационную систему персональных данных (ИСПДн) к тому или иному уровню защищенности необходимо[15]:

1. Определить категорию обрабатываемых персональных данных:

• *категория 4* - обезличенные и (или) общедоступные персональные данные;

• *категория 3* - персональные данные, позволяющие идентифицировать субъекта персональных данных;

• *категория 2* - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

• *категория 1* - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

2. Определить объем персональных данных, обрабатываемых в информационной системе:

• *объем 3* - одновременно обрабатываются данные менее чем 1 000 субъектов персональных данных в пределах конкретной организации;

• *объем 2* - одновременно обрабатываются персональные данные от 1 000 до 100 000 субъектов персональных данных, работающих в отрасли экономики РФ, в органе государственной власти, проживающих в пределах муниципального образования;

• *объем 1* - одновременно обрабатываются персональные данные более чем 100

15 http://is.gd/mJUflU

000 субъектов персональных данных в пределах субъекта РФ или РФ.

3. По результатам анализа исходных данных типовой ИСПДн присваивается один из следующих уровней защищённости[16] (см. табл. 6):

- уровень защищенности *4 (УЗ-4)* - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных;
- уровень защищенности *(УЗ-3)* - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;
- уровень защищенности *(УЗ-2)* - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;
- уровень защищенности *1 (УЗ -1)* - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных.

Объем / Категория	**Объем 3** (<1 000, организация)	**Объем 2** (1 000-100 000, отрасль, город)	**Объем1** (>100 000, субъект Федерации)
Категория 4 (обезличенные, общедоступные)	Уровень защищенности 4	Уровень защищенности 4	Уровень защищенности 4
Категория 3 (идентификационные)	Уровень защищенности 3	Уровень защищенности 3	Уровень защищенности 2
Категория 2 (идентификационные и еще)	Уровень защищенности 3	Уровень защищенности 2	Уровень защищенности 1
Категория 1 (медицинские, социальные)	Уровень защищенности 1	Уровень защищенности 1	Уровень защищенности 1

Таблица 6: Категория обрабатываемых персональных данных

Ниже приведен перечень операционных систем, сертифицированных для обработки персональных данных.

16 Ранее применявшийся термин «класс защиты» в отношении ИСПДн теперь не используется.

	Объект сертификации	Уровень защищённости персональных данных			
		4	3	2	1
	Microsoft Windows XP Professional[17]				
	ALT Linux 4.0 Desktop Professional				
	Trustverse Linux XP Desktop 2008 Secure Edition				
	MS Windows Server 2008 Standard Edition Service Pack 2				
	Microsoft Windows Server 2008 Enterprise Edition				
	Microsoft Windows Server 2008 Enterprise Edition Service Pack 2				
	Операционная система Microsoft Windows 7 в редакциях «Профессиональная», «Корпоративная» и «Максимальная»				
	Операционная система Microsoft Windows 7 (SP1) в редакциях «Профессиональная», «Корпоративная» и «Максимальная»				
	Операционная система Microsoft Windows Server 2008 R2 (в т.ч. SP1)				
	Novell SUSE Linux Enterprise Server 10				
	Oracle Enterprise Linux 5 Update 2 в редакции x86_64				
	Novell SUSE Linux Enterprise Server 10 SP3				
	ROSA Linux 2011				
	«SUSE Linux EnterpriseServer 11 ServicePack 1				
	Операционная система Microsoft Windows 7 (SP1) OEM в редакции «Профессиональная»				
	Alt Linux СПТ 6				
	МСВСфера Server 5.2				
	Astra Linux Special Edition				

Таблица 7: Уровни защищённости при обработке персональных данных

В соответствии с составом и содержанием организационных и технических мер

17 Срок действия сертификата до 04.07.2014 г.

по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённых приказом **ФСТЭК от 18.02.2013 г. № 21**, для обеспечения 1 и 2 уровней защищенности персональных данных, а также для обеспечения 3 уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 2-го типа, применяются:

- средства вычислительной техники не ниже 5 класса (см. табл. 2) ;
- средства защиты информации, программное обеспечение которых прошло проверку **не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей** (см. табл. 1).

Таким образом, все операционные системы Microsoft Windows, не могут использоваться для построения информационных систем обработки персональных данных 1 и 2 уровня, как **не прошедшие сертификацию по контролю отсутствия недекларированных возможностей** (несмотря на имеющиеся сертификаты).

В этой связи возникает вопрос, как будет разрешено это противоречие для операционных систем Windows.

С одной стороны, действие сертификата не окончено, с другой стороны, требования нормативного документа вступают в противоречие с фактическим положением дел.

Известно, что на практике специалистами используется обход требований по уровню защищённости для информационных систем, требующих защиты 1 уровня, путём искусственного разделения баз данных (например, межсетевым экраном), в результате чего достигается снижение числа записей в базе данных, и, соответственно, снижаются требования к уровню её защищённости.

Такой подход, безусловно, крайне негативно сказывается на общей защищённости персональных данных россиян.

Группа компаний РЕЛЭКС и ОАО «НПО РусБИТех» завершили работы по тестированию СУБД ЛИНТЕР в среде операционной системы общего назначения **«Astra Linux Common Edition»**.

СУБД ЛИНТЕР – реляционная система управления базами данных, сертифицированная ФСТЭК России по 2 классу защиты информации от несанкционированного доступа (НСД) и по 2 уровню контроля отсутствия недекларированных возможностей (НДВ), разрешённая к использованию для обработки и хранения информации с грифом «совершенно секретно», в том числе в информационных системах персональных данных (ИСПДн) до 1-го класса включительно.

http://www.cybersecurity.ru/press/110667.html

Испытательная лаборатория ЗАО «НПО «Эшелон» успешно завершила инспекционный контроль ПАК «Соболь» во ФСТЭК России.

Обновление комплекса, в основном, касается поддержки двух новых операционных систем: Альт Линукс СПТ 6.0 и Astra Linux Special Edition.

Основные функции, реализуемые ПАК «Соболь»: идентификация и аутентификация пользователей с помощью персональных идентификаторов, контроль целостности (КЦ) программного и аппаратного обеспечения до загрузки операционной системы , защита от несанкционированной загрузки операционной системы со съёмных носителей информации, функционирование механизма сторожевого таймера; регистрация событий, связанных с безопасностью системы.

ПАК «Соболь» 3.0 соответствует требованию руководящего документа по 2-му уровню контроля на отсутствие недекларированных возможностей, может использоваться в автоматизированных

системах уровня защищенности до 1Б и при построении ИСПДн класса К1.

http://www.npo-echelon.ru/news/9471/

Подводя итог, в целом можно отметить, что существующая российская система сертификации в области защиты информации в целом позволяет гарантировать сохранность конфиденциальной информации, однако вместе с тем, имеет ряд существенных недостатков.

Например, выданные сертификаты действительны в течении указанного в нём периода времени, измеряемого годами. Вместе с тем, этот период никаким образом не соотносится с периодом официальной поддержки программного продукта со стороны производителя.

В частности, официальная поддержка Windows XP осуществляется компанией Microsoft до 08.04.2014 г., тогда как сертификат защищённости (см. табл. 2 и 7) данной операционной системы, выданный ФСТЭК, действителен до 04.07.2014 г. То есть, на тот момент, когда данная операционная система может быть скомпрометирована в результате реверсинжиниринга обновлений для операционных систем Windows 7, Windows 8, её надёжность будет подтверждаться формальным документов без каких-либо реальных на то оснований. При этом её производитель может отказаться от исправления выявленных ошибок.

Кроме того, действующая нормативно-правовая база существенно устарела и фактически не позволяет постоянно иметь безопасную (с точки зрения возможности своевременного устранения ошибок в программном обеспечении) и в то же время сертифицированную систему.

Так, каждое обновление безопасности для программного обеспечения влечёт обязанность прохождения нового инспекционного контроля или даже повторной сертификации, на что затрачивается месяцы.

К слову, в настоящее время ФСТЭК рассматривается вопрос выработки подхода по сохранению сертификации при своевременном обновлении программного обеспечения.

Надеюсь, что данная информация поможет руководителям государственных органов и государственных компаний быстрее сориентироваться в требованиях действующего законодательства в части используемых инструментов для защиты сведений, содержащих государственную тайну.