УДК 004

АНАЛИЗ СИСТЕМ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ, ИСПОЛЬЗУЕМЫХ НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

© 2016 Т.Г. Габричидзе, В.А. Куделькин, А.М. Зайцев, А.В. Болтовский, Т.Г. Лебедева

ЗАО «Интегра-С», г. Самара

Статья поступила в редакцию 27.01.2016

*Р*ассмотрено современное состояние информационной безопасности Российской Федерации в условиях информационного противоборства с иностранными государствами, некоторые из которых ведут с нею необъявленную кибернетическую войну. Подчеркнуто отставание отечественных информационных технологий, обусловившее серьезную зависимость многих систем управления информационными ресурсами страны от иностранных производителей компьютерной и телекоммуникационной техники, от их программного обеспечения. Приведены результаты анализа систем управления базами данных, используемых Российскими федеральными государственными информационными системами по состоянию на август 2015 года. Обоснована необходимость отказа от применения зарубежного программного обеспечения. Исследованы новые нормативные правовые акты, по сути запрещающие использование программ иностранного производства в российских государственных и муниципальных учреждениях, на соответствующих критически важных (потенциально опасных) объектах с 1 января 2016 года. Высказана и обоснована сомнительность в реальности реализации данного предписания законодателя в столь короткое время в условиях отставания отечественных информационных технологий и критического состояния предприятий национальных отраслей промышленности, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты информации. Обозначены факторы, сдерживающие развитие современных и надежных систем информационной безопасности страны. Подчеркнута необходимость разработки и внедрения единой концепции создания систем безопасности. Предложено определение аппаратно-программного комплекса «Безопасный город», которому в аспекте создания единой комплексной системы безопасности в звене: опасный объект — муниципальное образование — субъект — регион — федерация должно быть отведено достойное место. Высказано мнение о целесообразности принятия Национального стандарта РФ ГОСТ Р «Интегрированные интеллектуальные системы мониторинга и обеспечения безопасности распределенных объектов предприятий и территорий. Архитектура и общие технические требования к оборудованию и программным средствам», проект которого подготовлен авторами и представлен в Технический комитет по стандартизации для рассмотрения и принятия по существу. В целях эффективного противостояния информационным вызовам, исходящим от потенциальных противников России, предложена консолидация и активизация усилий всех ответственных компетентных государственных и частных структур для разработки, поэтапного создания и постоянного развития надежных отечественных информационных и коммуникационных технологий, технических и программных средств, полностью независимых от информационных систем, процессов и ресурсов иностранных государств.

Ключевые слова: информационная безопасность; федеральные государственные информационные системы; системы управления базами данных; информационные технологии; программное обеспечение; операционные системы; несанкционированный доступ к информационной инфраструктуре.

Сложная современная международная обстановка, связанная с попытками отдельных государств изолировать Россию от внешнего мира, а значит, нанести ей весомый политический и экономический урон, неизбежно влекущий за собой социальные потрясения, требует принятия экстренных мер по обеспечению национальной безопасности нашей страны, существенно зависимой от ее информационной безопасности. Причем под информационной безопасностью вполне обоснованно понимается состояние защищенности национальных интересов нашей державы «в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» [1], в условиях информационного противоборства с иностранными государствами, ведущими с нами необъявленную кибернетическую войну [2–4], актуализировавшую разработку многогранных теоретических и практических проблем национальной кибербезопасности [5–12]. Ситуация осложнена отставанием отечественных информационных технологий, обусловившим серьезную зависимость многих

Габричидзе Тамази Георгиевич, доктор технических наук, советник президента Консорциума «Интегра-С».
E-mail: zaovolga@integra-s.com
Куделькин Владимир Андреевич, президент ЗАО «Интегра-С».
Зайцев Александр Михайлович, генеральный директор ВНИИ «Специальные технологии», г. Москва.
Болтовский Андрей Витальевич, генеральный директор ООО «Промснабзащита», г. Москва.
Лебедева Татьяна Георгиевна, заместитель генерального директора ВНИИ «Специальные технологии», г. Москва.

систем управления информационными ресурсами страны от иностранных производителей компьютерной и телекоммуникационной техники, от их программного обеспечения (далее — ПО). В результате несанкционированный доступ к информационной инфраструктуре наших органов власти и управления все еще открыт, повышая их уязвимость в информационном противостоянии с нашими недоброжелателями, которая в свете 12-го по счёту Послания Президента Российской Федерации В.В. Путина Федеральному Собранию просто недопустима [13].

Таблица 1. Системы управления базами данных, на которых работают российские ФГИС

№ № п/п	Наименование СУБД	Число ФГИС	Доля ФГИС в %
1.	MS SQL Server	132	41,1
2.	Oracle Database	90	28,0
3.	My SQL (Oracle)	50	15,6
4.	Postgre SQL	31	9,7
5.	IBM Lotus Notes/Domino	10	3,1
6.	Firebird	9	2,8
7.	Ред База Данных (форк Firebird)	9	2,8
8.	MS Access	4	1,2
9.	IBM DB2	2	0,6
10.	ИРБИС64	2	0,6
11.	MongoDB	2	0,6
12.	Линтер-ВС	1	0,3
13.	SAP Sybase SQL Anywhere	1	0,3
14.	Pick D3	1	0,3
15.	1С: База данных	1	0,3
16.	MS FoxPro	1	0,3
17.	IBM AIX	1	0,3
18.	Собственная разработка	1	0,3

Примечание: сумма долей превышает 100%, ибо некоторые ФГИС используют больше, чем одну СУБД

Чтобы не быть голословными, приведем сведения, полученные аналитическим центром TAdviser Report при исследовании федеральных государственных информационных систем (далее — ФГИС). Установлено, что государственные органы нашей страны для управления своими базами данных, как правило, используют базовое ПО иностранного производства, чем фактически поддерживают технологическую зависимость от зарубежных фирм-производителей операционных систем, изначально имеющих в подавляющем своем большинстве закрытые исходные коды, несущие в себе скрытую потенциальную угрозу [14]. Это наглядно видно из табл. 1 и 2, в которых сотрудниками указанного Центра сгруппированы результаты анализа систем управления базами данных (далее — СУБД), используемых российскими ФГИС по состоянию на август 2015 года [15].

Как видим, в рейтинге СУБД, составленном аналитическим центром TAdviser Report по результатам исследования базового ПО, на котором построены российские ФГИС, первенствуют продукты Microsoft и Oracle. При этом MS SQL Server и Oracle Database используются в 132 и 90 ФГИС соответственно (из 348).

Из табл. 2 усматривается, что в 42 крупных (с числом пользователей более 1000) ФГИС (из 131) в роли лидирующей СУБД выступает программный продукт американской корпорации Oracle. Ее представительство в Российской Федерации в январе 2015 года объявило о получении сертификата Федеральной службы по техническому и экспортному контролю (ФСТЭК) России на программное обеспечение Oracle Database (11g R2) Enterprise Edition для комплекса Oracle Exadata [16]. Сертификат подтверждает, что Oracle Database 11g R2 Enterprise Edition для комплекса

Таблица 2. Системы управления базами данных, на которых работают крупные российские ФГИС

№ № п/п	Наименование СУБД	Число ФГИС	Доля ФГИС в %
1.	Oracle Database	42	36,8
2.	MS SQL Server	36	31,6
3.	My SQL (Oracle)	23	20,2
4.	PostgreSQL	14	12,3
5.	Firebird	5	4,4
6.	Ред База Данных (форк Firebird)	2	1,8
7.	IBM Lotus Notes/Domino	2	1,8
8.	MS Access	2	1,8
9.	IBM AIX	1	0,9
10.	IBM DB2	1	0,9
11.	MongoDB	1	0,9
12.	SAP Sybase SQL Anywhere	1	0,9
13.	Pick D3	1	0,9

Oracle Exadata с установленными опциональными компонентами Oracle Database Vault и Oracle Advanced Security является системой управления базами данных со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, и соответствует требованиям технических условий [16].

Вместе с тем современное программное обеспечение — сложнейший интеллектуальный продукт, при создании которого задействуются специальные программные средства разработки и системное ПО, как правило, значительно превышающее по объему и сложности аналогичные характеристики прикладного ПО. По этой причине верифицировать системное программное обеспечение крайне сложно, а в некоторых случаях практически невозможно, в связи с чем «ни одна организация-разработчик не гарантирует абсолютной надежности создаваемого программного продукта, фактически снимая с себя ответственность за последствия, к которым могут привести дефекты в программах» [14]. Причем, особую сложность представляет собой обнаружение дефектов, внесенных в программные продукты преднамеренно, на этапе их создания, для завоевания приоритетных позиций в кибервойне, набирающей с каждым днем свои обороты.

Таким образом, зависимость России от иностранных производителей программного обеспечения, подтвержденная приведенными в таблицах 1 и 2 данными, носит системный характер и крайне опасна для информационной безопасности нашего государства, его органов власти и управления, инфраструктура которых в подавляющем своем большинстве все еще находится под угрозой кибердиверсий и кибертерроризма [17].

Положение дел отягчает широкое использование зарубежного проприетарного ПО, имеющего закрытые исходные коды. Его наиболее типичными и массовыми представителями являются, например, операционные системы семейства Windows крупнейшей американской транснациональной компании Microsoft Corporation.

Более того, даже использование открытого программного обеспечения чужеземного производства, имеющего открытые исходные коды, отнюдь не отвечает коренным интересам нашей державы в аспекте укрепления ее информационной безопасности. В данном контексте уместно заметить, что вторая по величине получаемых доходов (после Microsoft) американская корпорация Oracle Corporation, также специализирующаяся на производстве ПО, вступила в полемику с Минобороны США, пытаясь убедить военное ведомство в необходимости отказа от использования открытого ПО в критически важных для страны системах [18].

Таким образом, налицо информационная экспансия России, фактически угрожающая ее информационным ресурсам.

Для наглядности отметим, например, что практически весь федеральный сегмент электронного правительства нашей страны расположен в двух Центрах обработки данных российской телекоммуникационной компании «Ростелеком» в Москве, а задействованные для этого информационные системы и оборудование частично: арендованы у этой компании либо принадлежат Министерству связи и массовых коммуникаций Российской Федерации (далее — Минкомсвязь России). При этом программно-аппаратная инфраструктура ключевых систем данного электронного правительства — Единого портала государственных услуг (ЕПГУ) и Системы межведомственного электронного взаимодействия (СМЭВ) — закупались в два этапа.

Первый этап относится к 2009 году, когда было приобретено:

– для ЕПГУ — более 20 серверов HP, несколько маршрутизаторов Cisco и систем хранения Hitachi вместе с СУБД Oracle;

– для СМЭВ — четыре блейд-сервера и ленточная библиотека Sun, сервер HP, дисковый массив Hitachi и коммутатор Brocade;

– в качестве программной шины — решение Oracle.

На втором этапе, протекавшем в 2010 году, расширение вычислительных мощностей в основном происходило за счет оборудования американской компании IBM, входящей в число крупнейших в мире производителей и поставщиков аппаратного и программного обеспечения. При этом инфраструктура ЕПГУ потребовала 26 новых серверов, а СМЭВ — 5.

Кроме того, с 2010 года техника IBM стала использоваться и в инфраструктуре Государственной автоматизированной информационной системы «Управление», портала государственных продаж, системы управления ведомственной информатизацией.

Примечательно, что как раз в 2010 году состоялось назначение на пост замминистра связи и массовых коммуникаций нашей страны И. И. Массуха, ранее в течение 13 лет работавшего в российском отделении IBM, где он дорос до должности директора департамента продаж в госсектор. Более того, именно он в 2010–2012 годах курировал в Минкомсвязи России электронное правительство [19], де-факто лоббируя, как нам представляется, интересы IBM, а значит, обеспечивая ее официальное внедрение в наше государственное информационное пространство.

В наши дни реальность деструктивного и противоправного воздействия ведущих иностранных государств и компаний на элементы нашей национальной критической информационной инфраструктуры российским законодателем уже осознана. Об этом свидетельствует факт издания новых нормативных правовых актов, по сути запрещающих использование всех про-

грамм иностранного производства в российских государственных и муниципальных учреждениях с 1 января 2016 года. Это:

Ø Федеральный закон от 29.06.2015 № 188-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и статью 14 Федерального закона "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [20];

Ø постановление Правительства Российской Федерации от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» [21].

Первый нормативный правовой акт, обязывающий подтверждать происхождение используемых в нашей стране программ из Российской Федерации, а также расширять их применение и оказывать государственную поддержку нашим правообладателям программного обеспечения, дополнил действующую редакцию Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [22] статьей 12^1. Она посвящена особенностям государственного регулирования в сфере использования российских программ для электронных вычислительных машин и баз данных. В данной норме Закона описана процедура создания единого реестра отечественного программного обеспечения, а также приведены правила его формирования, устанавливаемые Правительством Российской Федерации. В ней также указано, что уполномоченный Правительством России федеральный орган исполнительной власти наделяется правом:

– допуска к формированию и ведению этого реестра специального оператора — организации, зарегистрированной на территории Российской Федерации, то есть находящейся в сфере ее юрисдикции;

– утверждения классификатора программ для электронных вычислительных машин и баз данных, на основании которого планируется формировать реестр.

Согласно данному Закону, «отечественными» могут считаться только программы, исключительные права на которые принадлежат самой Российской Федерации, ее гражданам либо организациям, к управлению которыми иностранцы доступа не имеют. Закон допускает участие в создании отечественного ПО коммерческих структур, но при условии, что российское участие в них составляет более 50%. В реестр однозначно не может быть включено программное обеспечение, сумма лицензионных выплат за рубеж по которому составляет более 30% от выручки правообладателя.

Более того, Федеральный закон от 29.06.2015 № 188-ФЗ изложил часть 3 статьи 14 Федерального закона от 5 апреля 2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [23] в новой редакции. В соответствии с ней, Правительству Российской Федерации предоставлено право запрещать допуск к участию в закупках программного обеспечения, отличного от отечественного.

Второй нормативный правовой акт (постановление Правительства РФ от 16.11.2015 № 1236) издан в порядке исполнения Федерального закона от 29.06.2015 № 188-ФЗ. Одновременно с ним этим же постановлением утверждены:

- «Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных»;
- «Порядок подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» [21].

Разумеется, запрет пока не будет касаться частных лиц и коммерческих структур. Однако в государственных учреждениях и на критически важных (потенциально опасных) государственных объектах путь для использования иностранных программ с 1 января 2016 года объявлен перекрытым в законодательном порядке.

Другой вопрос — реальность реализации данного предписания законодателя в столь короткое время в условиях отставания отечественных информационных технологий и критического состояния предприятий национальных отраслей промышленности, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты информации. При этом если некоторый прикладной софт в России все-таки разрабатывается, то ситуация с операционными системами (далее — ОС) очень проблематична, так как ни одна из них не является российской. Например, исключительные права на семейство ОС Windows принадлежат ранее упомянутой американской компании Microsoft Corporation, на ОС iOS и Mac OS — американской корпорации Apple, а альтернативная им ОС Linux разрабатывается интернациональным сообществом свободных разработчиков, доля россиян в котором весьма незначительна. Даже ОС Android, созданная американской транснациональной корпорацией Google, базируется на ядре Linux [24].

При таких обстоятельствах оперативный переход (до 1 января 2016 года) всех органов власти и управления, а также критически важных (потенциально опасных) государственных объектов нашей страны на программное обеспечение российского производства представляется спорным. Однако нацеленность нашего законодателя на обязательный их перевод в режим использования исключительно российских прикладных и

системных программных продуктов заслуживает полного понимания, особенно — в контексте обеспечения национальной безопасности. При этом в аспекте построения современных и надежных систем безопасности нашего государства нельзя не учитывать наличие ряда сдерживающих факторов, среди которых особо отметим:

– разобщенность действий участников процесса, обусловленную отсутствием стандартов и нормативных документов, устанавливающих общие и частные требования к разработке, производству и эксплуатации указанных систем;

– межведомственную несогласованность действий органов власти и управления, а также предприятий, организаций и учреждений в данном вопросе;

– серьезную зависимость процесса развития средств и систем безопасности от коммерческих интересов участников рынка, подчас сопряженную с коррупционной составляющей;

– необоснованное (с точки зрения унификации) применение закрытых протоколов обмена данными между оборудованием отдельных производителей;

– слабое развитие в стране института применения электронных подписей для идентификации данных и доступа к ним [25];

– стратегически ущербно построенные (значит, экономически необоснованные) действующие в стране ведомственные и региональные системы безопасности, которые все еще разобщены и не структурированы в едином контексте в связи с разнородностью подходов при изначальном определении их архитектуры.

Главное, что эти негативные факторы имеют место на фоне отсутствия в стране единой концепции создания систем государственной безопасности, а, следовательно, неэффективных многомиллиардных «целевых» трат из государственных и региональных бюджетов, из средств государственных и частных корпораций.

В свое время в порядке исполнения требований распоряжения Правительства Российской Федерации от 17.12.2010 № 2299-р, утвердившего план перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения на 2011– 2015 годы [26], и с учетом п. 5.1 ГОСТ Р 22.1.12-2005 [27] нами создан проект Национального стандарта РФ — ГОСТ Р «Интегрированные интеллектуальные системы мониторинга и обеспечения безопасности распределенных объектов предприятий и территорий. Архитектура и общие технические требования к оборудованию и программным средствам». Этот проект стандарта после получения замечаний и их устранения представлен в Технический комитет по стандартизации (в ТК-22 «Информационные технологии» и в подкомитет ПК-125 «Взаимосвязь оборудования для информационных технологий») для рассмотрения и принятия по существу.

Думается, что при положительном решении вопроса данный стандарт будет способствовать созданию единой комплексной системы безопасности в звене: опасный объект — муниципальное образование — субъект — регион — федерация. Естественно, что в этой системе достойное место должен занять аппаратно-программный комплекс «Безопасный город» [28]. Под ним мы понимаем комплексную систему безопасности на основе непрерывного мониторинга по сбору, обработке, документированию (архивированию) и передаче информации в едином информационном поле, позволяющем:

а) работать под управлением российских операционных систем с открытым исходным кодом;

б) иметь возможность импорта картографических данных и их общепринятых обменных форматов;

в) объединять все подсистемы безопасности в единую геоинформационную систему;

г) отображать объекты на 2D или 3D плане местности в 3D изображении самого объекта с размещением всех систем безопасности и с возможностью контроля во времени (4D);

д) осуществлять защиту информации с помощью соответствующей системы безопасности с грифом секретности, подтвержденным электронной подписью;

е) передавать в дежурно-диспетчерские службы опасных объектов, единые дежурно-диспетчерские службы муниципальных образований, центры управления в кризисных ситуациях (ситуационные центры министерств, ведомств, организаций) различных уровней информацию по оценке обстановки для принятия управленческих решений, связанных:

– с привлечением сил и средств Российской системы предупреждения и ликвидации чрезвычайных ситуаций при организации защиты населения и территорий;

– с их всесторонним финансовым и материально-техническим обеспечением.

Итак, для эффективного противостояния информационным вызовам, исходящим от наших потенциальных противников, необходима консолидация и активизация усилий всех ответственных компетентных государственных и частных структур для разработки, поэтапного создания и постоянного развития надежных отечественных информационных и коммуникационных технологий, технических и программных средств, полностью независимых от информационных систем, процессов и ресурсов иностранных государств.

В противном случае законодательный запрет на допуск программного обеспечения, происходящего из иностранных государств, останется благим намерением, всего лишь создавшим бла-

гоприятную почву для проведения соответствующих прокурорских проверок в порядке надзора и осуществления прокурорского реагирования за неисполнение либо ненадлежащее воли законодателя по рассмотренному вопросу.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ 09.09.2000 № Пр-1895. [Электронный ресурс]. URL: http://base.consultant.ru/cons/cgi/online.cgi?base=LAW&n=28679&req=doc (дата обращения: 13.12.2015).
2. Антонович П.И. О сущности и содержании кибервойны // Военная мысль. 2011. № 7. С. 39–46.
3. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны — реальная угроза национальной безопасности? / Ин-т проблем междунар. безопасности РАН. М.: КРАСАНД, 2011. 96 с.
4. Смирнов А. «Snowdengate»: анализ «цифрового фашизма» спецслужб США и их союзников // Информационная безопасность России: аналит. сб. / Редакция журнала «Бизнес и безопасность в России». 2014. Вып. 1. С. 105–120.
5. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 5 (8). С. 39–42.
6. Безкоровайный М.М., Татузов А.Л. Кибербезопасность — подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). С. 22–27.
7. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 1) // Вопросы кибербезопасности. 2013. № 1 (1). С. 2–9.
8. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 2) // Вопросы кибербезопасности. 2014. № 1 (2). С. 5–12.
9. Гришин С. Е., Седышев С. Г. Кибербезопасность и проблема повышения качества управления информацией // Вестник Саратовского государственного социально-экономического университета. 2012. № 1. С. 202–206.
10. Згоба А.И., Маркелов Д.В., Смирнов П.И. Кибербезопасность: угрозы, вызовы, решения // Вопросы кибербезопасности. 2014. № 5 (8). С. 30–38.
11. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1 (1). С. 10–16.
12. Стельмах А.П., Тонконогов А.В. Обеспечение кибернетической безопасности Российской Федерации: (основы общей киберологии): монография. М.: Изд-во РГАУ – МСХА им. К.А. Тимирязева, 2012. 102 с.
13. Мы не имеем права быть уязвимыми: Послание Президента России Владимира Путина Федеральному Собранию // Российская газета – Федеральный выпуск. 2015. 4 декабря. № 275 (6846). С. 1–4.
14. Малюк А. Скрытые угрозы зарубежного программного обеспечения. [Электронный ресурс]. URL: http://www.rusnevod.com/cgi-bin/rnev/start.cgi?grp=0114&prn1=info7 (дата обращения: 13.12.2015).
15. Какие СУБД используют федеральные органы власти России: отчет аналитического центра TAdviser Repor. [Электронный ресурс]. URL: http://www.tadviser.ru/index.php (дата обращения: 14.12.2015).
16. Платформа Oracle Database на Oracle Exadata сертифицирована ФСТЭК России. [Электронный ресурс]. URL: http://www.mskit.ru/news/n177573/ (дата обращения: 14.12.2015).
17. Варфоломеев А.А. Кибердиверсия и кибертерроризм: пределы возможностей негосударственных субъектов на современном этапе // Военная мысль. 2012. № 12. С. 3–11.
18. Oracle: «Открытому коду не место в оборонных системах». 2013. 17 октября. [Электронный ресурс]. URL: http://www.itshop.ru/Oracle-Otkrytomu-kodu-ne-mesto-v-oboronnyh-sistemah/l9i34926 (дата обращения: 14.12.2015).
19. Электронное правительство России. Полное досье // CNews: издание о высоких технологиях. 2013. 20 ноября. [Электронный ресурс]. URL: http://www.cnews.ru/articles/elektronnoe_pravitelstvo_rossii_polnoe_dose/1 (дата обращения: 15.12.2015).
20. Федеральный закон Российской Федерации от 29.06.2015 № 188-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статью 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» // Российская газета — Федеральный выпуск № 6716. 2015. 6 июля. С. 14.
21. Постановление Правительства Российской Федерации от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд». [Электронный ресурс]. URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n= 189116;fld=134;dst=1000000001,0;rnd=0.2992468161974102 (дата обращения: 16.12.2015).
22. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (действующая редакция). [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 17.12.2015).
23. Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (действующая редакция). [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_law_144624/ (дата обращения: 18.12.2015).
24. Путин запретил иностранное ПО в России // Арсеньевские вести. № 50 (1187). 2015. 8 июля. [Электронный ресурс]. URL: http://www.arsvest.ru/rubr/2/26720 (дата обращения: 19.12.2015).
25. Куделькин В.А., Пономарев В.Н. За безопасное будущее России: обращение Консорциума «Интегра-С» и ТК «Комплексная безопасность промышленности и энергетики» // OHRANA.RU. 2015. 4 февраля. [Электронный ресурс]. URL: http://ohrana.ru/articles/63926/ (дата обращения: 20.12.2015).

26. Распоряжение Правительства Российской Федерации от 17.12.2010 № 2299-р «Об утверждении плана перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения на 2011–2015 годы». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_111346/ (дата обращения: 21.12.2015).
27. ГОСТ Р 22.1.12-2005 «Безопасность в чрезвычайных ситуациях. Структурированная система мониторинга и управления инженерными системами зданий и сооружений. Общие требования» (в редакции от 01.06.2011). [Электронный ресурс]. URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=515303 (дата обращения: 21.12.2015).
28. Распоряжение Правительства Российской Федерации от 03.12.2014 № 2446-р «Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_172077/ (дата обращения: 22.12.2015).

ANALYSIS OF DATABASE MANAGEMENT SYSTEMS, USED IN THE RUSSIAN FEDERATION

© 2016 T.G. Gabrichidze, V.A. Kudelkin, A.M. Zaitsev, A.V. Boltovskii, T.G. Lebedeva

Consortium «Integra-S», Samara

The article deals with the current state of the information security of the Russian Federation in the conditions of information warfare with foreign countries, some of which lead to her undeclared cyberwar. It underlined the backlog of domestic information technology has caused a serious dependence of many information management systems of the country from foreign manufacturers of computer and telecommunication equipment, from their software. Results of the analysis of database management systems, used by the Russian federal government information systems as of August 2015. The necessity of renunciation of the use of foreign software. Explore new legal acts, in effect prohibiting the use of foreign-made programs in Russian state and municipal authorities, within the appropriate critical (potentially dangerous) objects to January 1, 2016. Expressed and grounded in the reality of dubious implementation of the provisions of the legislator in such a short time in a backlog of domestic information technologies and the critical state of national industries companies that develop and produce means of informatization, telecommunications and data protection. The factors constraining the development of advanced and reliable systems of information security. It stressed the need to develop and implement a unified concept of a safety system. A definition of hardware and software complex «Safe City», which in terms of creating a single integrated security system in the chain: a dangerous object — the municipality — the subject — the region — the federation should be given its rightful place. The opinion on the desirability of national standards GOST R «Integrated intelligent monitoring and security of distributed objects of enterprises and territories. Architecture and general technical requirements for equipment and software», drafted by the authors and submitted to the Standardization Technical Committee for consideration and decision on the merits. In order to deal effectively with information and communication challenges posed by potential enemies of Russia, proposed the consolidation and intensification of the efforts of all the responsibility of the competent public and private entities for the development, phased creation and continuous development of reliable national information and communication technology, hardware and software, completely independent of the information system, processes and resources of foreign countries.
Keywords: Information Security; Federal government information systems; database management systems; Information Technology; software; OS; unauthorized access to the information infrastructure.

Tamazi Gabrichidze, Doctor of Technics, Advisor to the President of the Consortium «Integra-S».
E-mail: zaovolga@integra-s.com
Vladimir Kudelkin, President of the Consortium «Integra-S».
Alexandr Zaitsev, General Manager, Moscow.
Andrey Boltovskii, General Manager, Moscow.
Tamara Lebedeva, Deputy General Manager, Moscow.

Сдано в набор 25.02.2015 г. Подписано к печати 17.03.2015 г. Формат бумаги 60x801/8
Офсетная печать Усл. печ. л. 20,3 Усл. кр-отт. 7,2 Уч-изд.л. 15,9 Тираж 200 экз. Зак.

Отпечатано в типографии АНО «Издательство СНЦ», 443001, Самара, Студенческий пер., 3а