

## **Обеспечение электронного суверенитета органов власти и местного самоуправления РФ при помощи свободного программного обеспечения**

**Каратов Марат Абдуллаевич**, СЗИУ РАНХиГС, факультет государственного и муниципального управления, студент 4 курса, marat.karatov@reactos.org

**Научный руководитель**

**Берштейн Василий Сергеевич**, СЗИУ РАНХиГС, доцент, кандидат социологических наук

### **Аннотация**

Сегодня человечество может наблюдать накаленную геополитическую обстановку во всем мире, касающуюся и Российскую Федерацию. Тенденции США, стран Европейского союза, к проведению политики санкционной блокады, направленной против нашей страны еще больше стимулирует нас к решению особо важных задач, касающихся непосредственного, действенного импортозамещения во всех сферах жизнедеятельности РФ. Крайне важно стоит отнестись к сфере информационных технологий, ведь от информационной, электронной безопасности, зависит стратегическая безопасность государства, и его суверенность в целом. Важно предпринять все возможное для реализации информационной независимости, как всей страны в целом, так и ее граждан в частности. Большинство людей по всей Земле, «рядовые» граждане, органы государственной власти и местного самоуправления Российской Федерации являются пользователями фактически одного семейства операционной системы (ОС), основывающей электронное функционирование вышеперечисленных структур, обеспечение их информационной безопасности.

В мире, в том числе, и в нашей стране наблюдается тенденция крупных компаний, органов власти, государственных корпораций, и частных лиц по переходу на свободное и бесплатное программное обеспечение (СПО). Эти действия обусловлены желанием избавиться себя от лицензионных расходов, шпионажа со стороны иностранных спецслужб и в целом желанием быть информационно независимыми. Простые пользователи и представители различных структур особо обеспокоены должным уровнем обеспечения информационной, электронной безопасности своих электронно-вычислительных машин. Страны Европы уже смогли убедиться в необходимости перехода не только учебных учреждений, но и государственных структур на СПО. Однако удовлетворить необходимым требованиям ни одной свободной системе не удалось, более того, на мировом рынке ОС отсутствует система, способная решить указанные проблемы. Для нашей страны выбор операционной системы для работы органов власти, учебных и медицинских учреждений стоит особо остро, ведь сегодня Россия находится в зависимости от иностранной продукции по многим пунктам, в том числе в софтверном сегменте. Важно иметь возможность обеспечить информационную безопасность наших органов государственной власти, так как их защита представляет собой защиту государства.

**Ключевые слова**

Свободное программное обеспечение, импортозамещение, органы власти, органы местного самоуправления, электронная и информационная безопасность, стратегическая безопасность, суверенитет государства

**Ensuring Electronic Sovereignty of Authorities and Local Self-Government of the Russian Federation with the Help of Free Software**

**Marat A. Karatov**, NWIM RANEPА, The Department of State and Municipal Administration, 3 curriculum, marat.karatov@reactos.org

**Abstract**

Today, humanity can observe a tense geopolitical situation in the world concerning the Russian Federation. Trends in USA, European Union countries, a policy of various sanctions blockade against our country further stimulates us to the solution of critical tasks relating to immediate, actionable import substitution in all spheres of life in Russia. It is extremely important you should treat the field of information technology, because information, e-security depends on strategic security of the state and its sovereignty as a whole. It is important to take all possible steps for implementation of informational independence, as the whole country and its citizens in particular. Most of the people in all the Earth, "ordinary" citizens, bodies of state power and local self-government of the Russian Federation are users are actually the same family of the operating system (hereinafter OS) based on the electronic functioning of these structures, ensuring their information security.

In the world, including in our country there is a trend of large companies, authorities, public corporations, and private individuals for the transition to open source and free software (hereinafter FOSS). These actions are driven by the desire to rid themselves of the licensing costs of espionage by foreign intelligence services and in General desire to be independent information. Ordinary users and representatives of the various bodies particularly concerned about the appropriate level of security of information, electronic security on their computers. European countries have been able to determine the necessity of transition not only educational institutions, but also state structures on SPO. However, to satisfy the necessary requirements any free the system has failed, moreover, in the global OS market, there is no system that can solve these problems. For our country the choice of operating system for the work of governments, educational and medical institutions is particularly acute, because today Russia is dependent on foreign products on many points, including in the software industry. It is important to have the ability to ensure information security of our state authorities, as their protection is a protection of the entire state.

**Keywords**

Free software, import substitution, the authorities, bodies of local self-government, and electronic information security, strategic security, the sovereignty of the state

Целью данной статьи является анализ возможности перехода органов государственной власти, местного самоуправления РФ с проприетарного (закрытого) на свободное программное обеспечение (открытое).

На данный момент осуществление работы фактически любого современного компьютера состоит из совокупного взаимодействия трёх основополагающих неотъемлемых частей:

- операционной системы;
- аппаратного обеспечения;
- прикладного программного обеспечения (далее – ПО);

В случае выявления какой-либо неисправности или недостаточного уровня функциональности любой из данных частей, две остальные становятся бесполезными. Следовательно, важно обеспечивать комплексное оснащение ЭВМ всеми необходимыми комплектующими, реализующими полноценную надежную работу компьютера.

Тематика информационной и сетевой безопасности целых стран последнее время вышла на первый план. Причина тому контроль над разработкой всевозможных программных продуктов, в особенности системного программного обеспечения, используемого на более чем 90 процентах компьютеров во всем мире, практически реализуется спецслужбами одного иностранного государства. Спецслужбы способны намеренно оказывать давление на производителей программного обеспечения с целью тайного внедрения последними в свои популярные продукты вероятных программных уязвимостей. В случае возникновения неблагоприятных геополитических условий союзничества или напряженности между государствами подобные уязвимости скорее всего будут использованы с целью осуществления информационных диверсий и шантажа в масштабах всей страны.

Заявления о реалистичности подобного сценария не раз озвучивались за последние два десятилетия различными независимыми друг от друга аналитиками информационной безопасности. Секретарь комиссии Совета Федерации РФ по развитию информационного общества А. Шепилов в конце апреля 2014 г. на форуме РИФ+КИБ озвучил предложение разработать новую стратегию информационной и кибернетической безопасности страны, а также создать собственную национальную операционную систему, способную обеспечить информационную, электронную безопасность граждан, органов государственной власти России. По его словам, Москве следует позаботиться о создании национальной операционной системы, которая обеспечит страну «цифровым суверенитетом». Это предложение особо актуально, ведь из-за действия против России западных санкций Microsoft, Oracle, Symantec и HP уже заявили о готовности отключить российские банки, попавшие в санкционный список США, от своих программных продуктов.

Актуальность данной темы заключается в том, что еще задолго до введения так называемых санкций странами Европейского союза и США против нашей страны, Правительство РФ во главе с В. В. Путиным от 17 декабря 2010 г. вынесло распоряжение № 2299-р, в рамках которого стояла задача утвердить предлагаемый план перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения на 2011–2015 гг.<sup>1</sup>

К сожалению, данное распоряжение не было реализовано. Также В. В. Путиным был подписан закон 29 июня 2015 г. № 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», предусматривающий создание реестра российских программ, а также возможность ввода ограничений на ис-

---

<sup>1</sup> URL: <http://minsvyaz.ru/common/upload/2299p.pdf>. Распоряжение Правительства от 17 декабря 2010 г. № 2299-р.

пользование зарубежных товаров и услуг с 1 января 2016 г.<sup>2</sup> Фактически в то же время Минкомсвязи внесло в Правительство проект постановления с аналогичными юридическими нормами. Процесс импортозамещения в целом сегодня несет не рекомендательный, а обязательный характер для любого развитого государства, для нашего в особенности. Ведь сложно представить, каков будет негативный для страны результат бездействия и стагнации отечественного производства в отрасли военно-промышленного, аграрно-промышленного комплексов, не станет в этом списке исключением и информационно-технологический сегмент.

Существует большое количество разработчиков, производителей аппаратного обеспечения различного уровня в Китае, США, Европе, России – AMD, Intel, HP, Dell, Rover Computers, Prestigio и некоторые другие организации. Тем самым за последние десятилетия определенными разработчиками были осуществлены разработки, поддерживаемые и распространяющиеся миллионами единиц прикладного ПО. Количество производителей ПО в разы превышает количество производителей аппаратного обеспечения, в свою очередь, их география гораздо шире. Следовательно, можно сказать, что в сфере аппаратного и программного обеспечения есть важная и необходимая конкуренция между производителями, обеспечивающая стабильное развитие отрасли, предлагаемый ассортимент, свободу выбора для потребителей и стратегическую безопасность пользователя и любого государства.

В сфере операционных систем сложилась специфическая ситуация. Существует всего одна, имеющая особенно широкое распространение, операционная система Windows компании Microsoft (США), занимающая по числу установок и пользователей практически монопольное положение на мировом рынке ОС. Продукты конкурентов предполагают либо полную замену компьютера и прикладного программного обеспечения (в случае с продукцией фирмы Apple), либо замену уже имеющегося всего комплексного программного обеспечения и определенной части несовместимого аппаратного обеспечения (в случае с операционными системами на базе Linux).

Операционные системы семейства Windows обладают рядом важных недостатков. Системные требования растут с каждой последующей версией, приводя к необходимости покупки нового дорогостоящего аппаратного обеспечения и совокупных устройств с более высокой производительностью заблаговременно до планируемого выхода из строя аналогичных изделий, приобретенных ранее. Разработку опосредовано контролирует Правительство США, так как компания Microsoft является американской. Юридически и технические сложные схемы лицензирования, практикуемые корпорацией, во многих случаях делают из клиентов невольных пользователей платформы и заставляют последних нести значительные расходы, связанные с приобретением фирменного ПО. Закрытые исходные коды делают невозможным полноценный аудит безопасности применения ОС данного семейства для всех желающих и дают повод подозревать наличие встроенных шпионских модулей и «потайных ходов» встроенных под давлением спецслужб. Данные подозрения многократно косвенно подтверждались различными утечками внутренних документов Агентства Национальной Безопасности США, к примеру, как это произошло во время «шпионского» скандала, инициированного Эдвардом Сноуденом. Важно:

- обеспечить импортозамещение проприетарных компонентов информационных систем, снизить зависимость от иностранных монополистов;
- стимулировать развитие отечественной отрасли разработки программ для ЭВМ;

<sup>2</sup> URL: <http://kremlin.ru/acts/bank/39838>. Федеральный закон от 29.06.2015 г. № 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».

- расширить возможности участия отечественных разработчиков в выполнении работ и оказании услуг для государственных и муниципальных нужд, обеспечивая дополнительные инвестиции в развитие отечественного производителя;
- обеспечить высокого уровня технологическую независимость;
- уменьшить число нарушений, связанных с правовой защитой программ.

Все эти пункты способно обеспечить свободное программное обеспечение, а именно предлагаемая мною операционная система ReactOS, имеющая возможность решения вышеупомянутых проблем, и создания условий для реализации комплексного процесса импортозамещения в ИТ, способной стать основой для создания фактически универсальной отечественной ОС Российской Федерации. Данная система была представлена первым лицам страны, отмечена профильным федеральным министерством, как система, имеющая один из наибольших уровней импортозамещающего потенциала, заняв 2 место в конкурсе от Минкомсвязи в сфере клиентских и серверных ОС. Являясь полностью бесплатной и свободной, созданной с нуля, совместимой на 99% с приложениями и программами семейства ОС Windows, ReactOS способна незаметно для обычного пользователя сменить иностранную операционную систему, обеспечив тем самым информационный, электронный суверенитет, как простых граждан, так и органов государственной власти и местного самоуправления.<sup>3</sup>

Таким образом, можно сделать вывод, что использование проприетарных операционных систем иностранного производства, а именно США, имеющих на сегодня фактически абсолютное монопольное положение на мировом рынке ОС, несет в себе потенциальную угрозу информационной безопасности отдельных лиц, организаций и органов власти в целом, в виде глобального процесса осуществления шпионажа, диверсий и провокаций. Однако, открытые операционные системы, имеющиеся на рынке, не способны обеспечить органы государственной власти и местного самоуправления своими качественными характеристиками и надежностью. Тем не менее, имеется стойкая тенденция перехода на СПО. По результатам выявленного противоречия в виде несоответствия спроса и предложения, неспособности обеспечения электронного суверенитета местного самоуправления и органов власти нашей страны, мною предложено решение проблем, связанных с информационной уязвимостью государственных органов России в виде реализации и внедрения открытой операционной системы ReactOS совместимой с программным и аппаратным обеспечением для платформы Windows. Считаю особо важным решение проблемы информационной безопасности страны, обеспечения должного уровня конкурентоспособности на мировой арене, развития информационно-технологической отрасли России, которая в свою очередь будет служить неким катализатором для социально-экономического развития, сделав Российскую Федерацию сильным и по-настоящему суверенным государством.

---

<sup>3</sup> URL: <http://www.reactos.org>. Официальный сайт ReactOS.