ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.056.5:004.738.5

Перспективы перехода госучреждений на импортонезависимое программное обеспечение в рамках соблюдения информационной безопасности

А.С. Казанцев А.И. Дубровина
Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Аннотация
Комплексное изменение технической архитектуры программного обеспечения в системе госучреждений, обеспечивающей обмен данными между интерфейсом сотрудников и устройствами сервера, представляет собой сложную задачу. С одной стороны, такой переход оказывает позитивное воздействие на развитие отечественной IT-индустрии и технологического сектора, способствует созданию новых рабочих мест, разработке новых защитных механизмов в сфере информационных технологий. Он позволяет упростить и ускорить множество автоматизированных процессов. Но, с другой стороны, по-прежнему актуальными при этом остаются вопросы безопасности и уязвимости автоматизированной информационной системы в условиях вредоносных воздействий. В настоящей статье проведен анализ процесса перехода на импортонезависимое программное обеспечение (ПО) и представлены мероприятия по его улучшению.

Ключевые слова: отечественное ПО, российские производители, импортонезависимая продукция, внедрение ПО, обучение сотрудников

Для цитирования. Казанцев А.С., Дубровина А.И. Перспективы перехода госучреждений на импортонезависимое программное обеспечение в рамках соблюдения информационной безопасности. *Молодой исследователь Дона.* 2024;9(3):32–35.

Prospects for the Transition of Government Agencies to Import-Independent Software in the Context of Information Security Compliance

Aleksandr S. Kazantsev, Angelina I. Dubrovina
Don State Technical University, Rostov-on-Don, Russian Federation

Abstract
A major change in the technical architecture of software used by government agencies, involving data exchange between employee interfaces and server devices, is a challenging task. On the one hand, this transition has a positive impact on the development of domestic IT industry and technology sectors, contributing to the creation of new jobs and development of new protection mechanisms in information technology. It allows for simplification and acceleration of many automated processes. On the other hand, it raises concerns about security and vulnerability of automated information systems to malicious attacks. The article explores the process of moving towards import-independent software and proposes measures to improve security.

Keywords: domestic software, Russian manufacturers, import-independent products, software implementation, employee training

For citation. Kazantsev AS, Dubrovina AI. Prospects for the Transition of Government Agencies to Import-Independent Software in the Context of Information Security Compliance. *Young Researcher of Don.* 2024;9(3):32–35.

Введение. В связи с введением санкций в виде ограничений и запрета на ввоз программных и технических средств в Россию, на предоставление услуг зарубежными компаниями перед отечественными производителями встал вопрос о переходе на собственные разработки. На российском рынке уже стали появляться новые ПО и оборудование, широкими темпами идёт продвижение продукции отечественных производителей, что в перспективе позволит полностью заменить экспортируемое из-за рубежа оборудование на российское, а это подчеркивает необходимость развития национальной инфраструктуры информационных технологий и снижения зависимости от иностранных поставок.

Осуществить мгновенный переход на отечественное ПО не представляется возможным в связи с несовместимостью новых операционных систем (ОС) и разработанного ПО, используемых в настоящее время в большинстве госучреждений. В связи с этим возникает потребность в частичном использовании решений производителей дружественных стран.

Цель данного исследования — провести анализ целесообразности и необходимости перехода на отечественное ПО как части долгосрочной стратегии цифровизации бизнеса. Задачи, которые для достижения поставленной цели решали авторы, состояли в разработке предложений по планированию автоматизации компаний, определению их стратегии и подходов к разработке IT-решений. Кроме того, проведена оценка рисков и представлен план перехода к цифровой независимости.

Основная часть. Преимущества перехода. Абсолютными преимуществами перехода на отечественное ПО являются следующие аспекты:

– переход на отечественное ПО может снизить зависимость от иностранных компаний и уменьшить риск санкций, которые влияют на доступ к зарубежным технологиям;

– использование отечественного ПО повысит уровень безопасности данных, так как они не будут передаваться за границу или подвергаться риску утечки [1];

– поддержка отечественного производителя будет способствовать дальнейшему развитию IT-индустрии и созданию новых рабочих мест;

– переход на отечественные продукты может стимулировать конкуренцию, и за счет этого будет повышаться качество разрабатываемого программного обеспечения;

– разработка и использование отечественного ПО требуют наличия квалифицированных специалистов, что может способствовать развитию IT-образования и повышению профессионализма разработчиков [2];

– переход на отечественный софт может стимулировать появление инноваций и разработку новых технологий в стране;

– в условиях экономических санкций переход на отечественное программное обеспечение является одним из способов импортозамещения и снижения зависимости от иностранных технологий;

– использование отечественного софта упрощает контроль и регулирование отрасли со стороны государства, так как все данные остаются внутри страны.

Введение в эксплуатацию импортонезависимого ПО приведёт к повышению уровня кибербезопасности, уменьшению количества утечек конфиденциальной информации, происходящих из-за уязвимости ПО зарубежных производителей. Национальные интересы и стратегические приоритеты закреплены в Стратегии национальной безопасности Российской Федерации [3]. Также внедрение импортонезависимого ПО оказывает положительное влияние на развитие отечественной IT-индустрии посредством создания новых рабочих мест и разработки новых защитных механизмов в области информационных технологий.

Требования для перехода. Для успешного импортозамещения в данной отрасли требуется:

1. Разработать и принять законодательные нормы и правила, стимулирующие отечественное производство и сдерживающие импорт. По данному поводу в 2022 году приняты указы Президента РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [4] и «О применении ответных специальных экономических мер в связи с недружественными действиями некоторых иностранных государств и международных организаций» [5].

2. Предоставить финансовые поощрения, субсидии, льготы или другие формы поддержки компаниям, активно занимающимся разработкой отечественного ПО/железа.

3. Осуществить поддержку образовательных и научных программ, направленных на подготовку квалифицированных специалистов в области информационной безопасности (ИБ).

4. Предоставить преимущества отечественным поставщикам, в частности, уменьшить налоги на поставки для стимулирования и использования отечественной продукции и услуг.

Приказом Минцифры России утверждены методические рекомендации по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации [6]. В 2018 году Минкомсвязи России издало приказ об утверждении методических рекомендаций по переходу органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления муниципальных образований Российской Федерации на использование отечественного офисного программного обеспечения, в том числе ранее закупленного офисного программного обеспечения [7].

5. Разработать долгосрочные стратегии развития отечественного производства с учетом технологических, экономических и социальных факторов.

Эти требования помогут создать благоприятную среду для развития отечественного производства и успешного импортозамещения.

Перемены в области защиты. До санкций (до 2019 года) экономика стремилась к стабильному росту, существовала зависимость от импорта в некоторых отраслях, но в целом рынок был открыт для иностранных поставщиков (красный уровень угрозы). На рис. 1 представлен график, на котором показаны изменения количества выявленных угроз и число отечественного ПО за период с 2019 по 2024 год [8, 9].

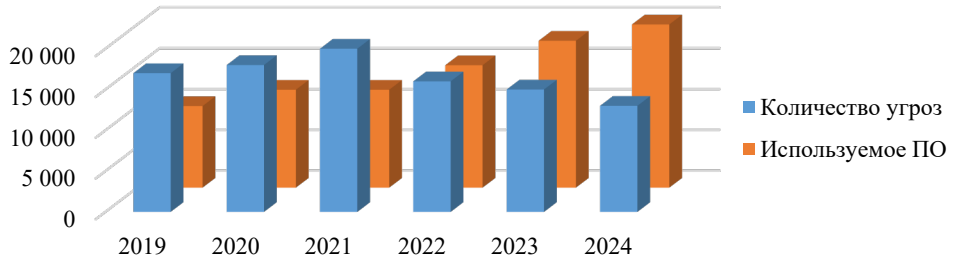

Рис. 1. График изменения количества выявленных угроз и числа отечественного ПО

По данным этого графика можно сделать вывод, что постепенно почти все государственные органы перешли на отечественное ПО, а количество угроз существенно уменьшилось.

Для мотивации специалистов в области развития информационных технологий должны быть предприняты следующие меры:

1. Предоставление специалистам возможности профессионального роста и обучения новым технологиям, связанным с отечественным производством.

2. Введение финансовых поощрений, бонусов или иных привилегий для специалистов, внесших значительный вклад в успешное импортозамещение.

3. Создание и поддержка инновационных сред с целью вдохновения и стимулирования творчества сотрудников.

4. Установление партнерских отношений с университетами и образовательными центрами для подготовки квалифицированных кадров.

5. Обеспечение прозрачной коммуникации относительно целей импортозамещения и важности роли специалистов в этом процессе.

6. Предоставление специалистам возможности участвовать в процессе принятия стратегических решений, повышая их ответственность и мотивацию.

Эти меры будут способствовать созданию стимулирующей среды, в которой специалисты могут принимать активное участие в процессе успешного импортозамещения.

Заключение. В настоящей работе рассмотрены целесообразность и необходимость проведения мероприятий по импортозамещению. Основными предложениями по планированию автоматизации компании, стратегии и подходами к разработке IT-решений являются:

1. Разработка стратегии информатизации (IT-стратегии): определение основных целей развития IT-инфраструктуры и плана мероприятий по их достижению.

2. Разработка концепции автоматизации: определение задач, связанных с внедрением корпоративных информационных систем, функциональных требований к системе и сравнительного анализа возможных программных решений.

3. Разработка технического задания: отражение функциональных и нефункциональных требований к системе, согласование с заказчиком и обеспечение единого понимания целей и функций внедряемой автоматизированной системы.

Оценка рисков и составление плана перехода к цифровой независимости включает в себя:

1. Анализ текущего состояния компании и выявление ключевых бизнес-процессов, требующих автоматизации.

2. Аудит IT-инфраструктуры для выявления взаимосвязей элементов инфраструктуры и бизнес-процессов.

3. Определение принципов выбора и последовательности внедрения корпоративных информационных систем.

4. Оценка стоимости и рисков проекта по внедрению системы, выбор поставщика и сравнение программных решений.

5. Формирование плана мероприятий по переходу к цифровой независимости, включая внедрение автоматизированных систем и обучение персонала.

На основании проведенного анализа можно сделать вывод, что целесообразность перехода на импортонезависимое ПО в России связана с рядом преимуществ и вызовов. Преимущества включают в себя снижение зависимости от иностранного ПО, возможность влиять на обновления ПО, развитие внутренних технологий, что также скажется на повышении уровня внутренней информационной безопасности страны. Однако имеются сложности, такие как отсутствие аналогов некоторых информационных систем и медленное развитие IT-продуктов в связи с низкой конкуренцией. Важно найти баланс между использованием отечественного ПО и сохранением качества работы информационных систем.

Список литературы

1. *О коммерческой тайне.* Федеральный закон № 98-ФЗ от 29.07.2004. URL: https://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 05.03.2024).

2. *О дополнительных мерах по обеспечению информационной безопасности Российской Федерации*. Указ Президента Российской Федерации № 250 от 01.05.2022. URL: https://www.garant.ru/hotlaw/federal/1541868/ (дата обращения: 05.03.2024).

3. *О Стратегии национальной безопасности Российской Федерации*. Указ Президента РФ № 400 от 02.07.2021. URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 05.03.2024).

4. *О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации*. Указ Президента РФ № 166 от 30.03.2022. URL: https://mvd.consultant.ru/documents/1057759 (дата обращения: 05.03.2024).

5. *О применении ответных специальных экономических мер в связи с недружественными действиями некоторых иностранных государств и международных организаций*. Указ Президента РФ № 252 от 03.05.2022. URL: https://www.consultant.ru/document/cons_doc_LAW_416210/ (дата обращения: 05.03.2024).

6. *Об утверждении Методических рекомендаций по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в Российской Федерации*. Приказ Минцифры России № 21 от 18.01.2023. URL: https://www.consultant.ru/document/cons_doc_LAW_439904/ (дата обращения: 05.03.2024).

7. *Об утверждении методических рекомендаций по переходу органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления муниципальных образований Российской Федерации на использование отечественного офисного программного обеспечения, в том числе ранее закупленного офисного программного обеспечения*. Приказ Минкомсвязи России № 335 от 04.07.2018. URL: https://www.consultant.ru/document/cons_doc_LAW_303138/ (дата обращения: 05.03.2024).

8. *Эксперты заявили о росте в три раза числа хакерских атак на игровой сегмент ИТ России*. URL: https://www.forbes.ru/tekhnologii/473177-eksperty-zaavili-o-roste-v-tri-raza-cisla-hakerskih-atak-na-igrovoj-segment-it-rossii (дата обращения: 05.03.2024).

9. *DDoS-атаки в России*. URL: https://www.tadviser.ru/index.php/ (дата обращения: 05.03.2024).

Об авторах:

Александр Сергеевич Казанцев, студент кафедры вычислительных систем и информационной безопасности Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), aleks_kazanzev@mail.ru

Ангелина Игоревна Дубровина, ассистент кафедры вычислительных систем и информационной безопасности Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), adubrovina@yug.gkovd.ru

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the Authors:

Aleksandr S. Kazantsev, Student of the Department of Computer Systems and Information Security, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), aleks_kazanzev@mail.ru

Angelina I. Dubrovina, Assistant of the Department of Computer Systems and Information Security, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), adubrovina@yug.gkovd.ru

Conflict of interest statement: the authors do not have any conflict of interest.

All authors have read and approved the final manuscript.