УДК 004.056.5

Шаповалова В.А.,
студент
3 курс, факультет «Управление»
ЮРИУ РАНХиГС
Россия, г. Ростов-на-Дону

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РОССИЙСКОЙ ФЕДЕРАЦИИ В СОВРЕМЕННЫХ РЕАЛИЯХ

Аннотация: *В статье исследуется состояние информационной безопасности в России. Анализируется современное состояние, выявляются тенденции развития в данной области. Приводятся существующие проблемы и указываются перспективы в данной сфере.*

Ключевые слова: *информация, информационное общество, информационные технологии, информационная безопасность, импортозамещение.*

Annotation: *The article examines the state of information security in Russia. The current state is analyzed, the tendencies of development in this area are revealed. The existing problems and prospects in this sphere are given.*

Keywords: *information, information society, information technologies, information security, import substitution.*

Характерной чертой развития и функционирования современного общества является его информатизация. Информационная сфера, в свою очередь, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации.

Национальная безопасность России, а именно защита национальных интересов информационной сфере существенным образом зависит от обеспечения

информационной безопасности, в чем и состоит актуальность исследования, и в дальнейшем эта зависимость будет все больше возрастать [1].

Цель и методология исследования

Цель исследования – выявить и проанализировать существующие и планируемые направления деятельности в области осуществления информационной безопасности (далее – ИБ) в Российской Федерации в разрезе ориентира на импортозамещение.

В работе рассматриваются два аспекта обеспечения ИБ: программный и аппаратный с опорой на Распоряжение Правительства РФ от 01.11.2013 N 2036-р и Доктрину информационной безопасности Российской Федерации [2].

В ходе исследования были выявлены следующие направления реализации обеспечения ИБ в программном и аппаратном аспектах.

Результаты исследования

На практике «безопасность в информационном обществе» [3] реализуется достаточно успешно и эффективно. Итак, в области *программного* подхода к защите информации в разрезе учитываемых Доктриной национальных интересов достигнуты следующие результаты. Необходимо также отметить, что последние являются одним из ориентиров политики, указанных в вышеприведенном НПА: стимулирование деятельности предприятий, обеспечивающих ИБ.

1. По итогам девяти месяцев 2016 года продажи лицензий, подписок и сервисов «1С: Предприятия» выросли на 19% по сравнению с аналогичным периодом 2015 года. Одним из факторов данной динамики является защищенность и конфиденциальность данных в сравнении с зарубежными аналогами. Согласно Приказу Минкомсвязи, импортозамещение в сфере бизнес-приложений является первым пунктом.

2. Далее следует антивирусное программное обеспечение. Здесь уже наряду с важностью промышленного масштаба речь идет о защите конституционных прав и свобод каждого человека и гражданина, согласно Доктрине. В РФ широко распространено использование продуктов «Лаборатории Касперского», специализация которых состоит в защите индивидуальных и корпоративных

пользователей от компьютерных вирусов, спама, хакерских атак и прочих киберугроз, в чем данное отечественное ПО оптимально.

3. Как один из интернет-сервисов, применяемых в корпоративной среде в рамках реализации одного из направлений Приказа Минкомсвязи, можно выделить картографический сервис NextGIS Web (серверная Веб ГИС предназначенная для хранения, визуализации и организации многопользовательского доступа к геоданным).

4. Что касается мобильного ПО, вопрос о котором в разрезе ИБ и импортозамещения также поднимается в Приказе, то в Сколково была разработана отечественная операционная система для мобильных устройств Tizen, для которой стало возможным по силе конкурировать с платформой Android [4].

5. Также поставкой продуктов, удовлетворяющих обеспечению ИБ и требованиям пользователей, занимается компания «Код безопасности» [5], предоставляющий средства защиты информации от несанкционированного доступа, межсетевые экраны, аппаратно-программных модули доверенной загрузки.

6. Переход на отечественное ПО в рамках Доктрины ИБ коснулся и технологического функционирования государственных организаций, как это указано в Приказе Минкомсвязи. В частности, до конца 2017 года переводу с систем управления базами данных Oracle на PostgreSQL будет подвержен единый портал госуслуг (ЕПГУ) [6].

Что касается *аппаратной* стороны обеспечения ИБ, то реализованы следующие проекты.

1. Для защиты информационной среды были созданы системы мониторинга и охраны «Волга», на базе российского DWDM-оборудования, и «Дунай». Системы информируют о приближении к охраняемому объекту и позволяют оперативно реагировать до осуществления врезки в магистраль.

2. Сетевая защита, как правило, обеспечивается установкой на границе сетей так называемых экранов. Примерами экранов являются такие, как аппаратные межсетевые экраны D-Link серии DFL, обладающие функцией проверки трафика

на наличие вредоносных программ; ALTELL NEO — российские аппаратные межсетевые экраны нового поколения, сертифицированные ФСТЭК на самые высокие классы защиты.

3. Одна из серьезных проблем в аппаратном обеспечении — процессор. Это самое технологически сложное устройство, безопасность которого трудно проверить, поэтому рациональнее использовать свои аналоги. Например, четырехъядерный микропроцессор «Эльбрус-4С».

4. НТЦ «Модуль» – высокопроизводительные процессорные ядра с архитектурой DSP/RISC.

5. «Аладдин Р.Д.» – средства информационной безопасности и защиты конфиденциальных данных.

6. Группа компаний «Микрон» – производитель и экспортер интегральных микросхем (смарт-карты, транспортные и другие RFID-карты, sim-карты, банковские карты с чипом, социальные карты и другие идентификационные документы).

7. «Т-Платформы» – суперкомпьютеры для высокопроизводительных вычислений, микропроцессор «Байкал» [7, с. 98].

Таким образом, на сегодняшний день сформулировано два базовых принципа информационной безопасности, которая должна обеспечивать:

- целостность данных – защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных;
- конфиденциальность информации и одновременно ее доступность для всех авторизованных пользователей.

Значение защиты информации в современном информационном обществе трудно переоценить, так как вышеуказанная проблема касается всех сфер государственной и общественной деятельности. Информацию в наше время можно сравнить с оружием: ее могут использовать для шантажа, она может стать причиной развязывания войны. Именно поэтому безопасность в информационном обществе рассматривается как одна из главных проблем современности.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // «Собрание законодательства РФ», 12.12.2016, № 50, ст. 7074.

2. Распоряжение Правительства РФ от 01.11.2013 № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года» // «Собрание законодательства РФ», 18.11.2013, № 46, ст. 5954.

3. Постановление Правительства РФ от 15.04.2014 № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011 – 2020 годы)» // «Собрание законодательства РФ», 05.05.2014, № 18 (часть II), ст. 2159.

4. Замещая импорт // Новости // В Сколково представлена готовая отечественная операционная система для мобильных устройств Tizen [Электронный ресурс] URL: http://zimport.ru/news/v-skolkovo-predstavlena-gotovaya-otechestv ennaya-operacionnaya-sistema-dlya-mobilnyx-ustrojstv-tizen/ (дата обращения: 26.06.2019).

5. Код безопасности [Электронный ресурс] URL: http://www.securitycode.ru/ (дата обращения: 26.06.2019).

6. TADWISER // Проект “Электронное правительство” (миграция с Oracle на PostgreSQL) [Электронный ресурс] URL: http://www.tadviser.ru/index.php/(Oracle_ PostgreSQL) (дата обращения: 26.06.2019).

7. Калюжный К.А. Состояние и перспективы импортозамещения в российской ИТ-отрасли // Наука. Инновации. Образование. – 2016. – №2. – С. 96-100.