ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДАННЫХ

Садовский В.Ю., Шепеленко В.Р.

Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники
г. Минск, Республика Беларусь

Савенко А.Г. – старший преподаватель, м.т.н.

Аннотация. В связи с тем, что белорусская экономика с каждым годом все больше интегрируется в мировую, абсолютно точно необходимо соблюдение международных требований конфиденциальности информации и защиты ресурсов информационных систем. В данной работе рассматриваются проблемы информационной безопасности.

Возможность проблемы информационной безопасности объясняется двумя основными причинами: ценностью накопленных информационных ресурсов и критической зависимостью от информационных технологий. Разрушение важной информации, кража конфиденциальных данных, перерыв в работе вследствие отказа – все это выливается в крупные материальные потери, наносит ущерб репутации организации. Проблемы с системами управления или медицинскими системами угрожают здоровью и жизни людей.

Современные информационные системы (ИС) сложны и, значит, опасны уже сами по себе, даже без учета активности злоумышленников. Постоянно обнаруживаются новые уязвимые места в программном обеспечении. Приходится принимать во внимание чрезвычайно широкий спектр аппаратного и программного обеспечения, многочисленные связи между компонентами.

Меняются принципы построения корпоративных ИС. Используются многочисленные внешние информационные сервисы; предоставляются вовне собственные; широкое распространение получил аутсорсинг, когда часть функций корпоративной ИС передается внешним организациям. Развивается программирование с активными агентами.

Подтверждением сложности проблематики информационной безопасности является параллельный (и довольно быстрый) рост затрат на защитные мероприятия и количества нарушений информационной безопасности в сочетании с ростом среднего ущерба от каждого нарушения.

Успех в области информационной безопасности может принести только комплексный подход, сочетающий меры шести уровней [1]:

– морально-этнические;
– правовые (законодательные);
– технологические;
– организационные (процедурные, административные);
– физические
– технические (программные, аппаратные, программно-аппаратные)

Проблема информационной безопасности – не только техническая. Без законодательной базы, без постоянного внимания руководства организации и выделения необходимых ресурсов, без мер управления персоналом и физической защиты решить ее невозможно. Комплексность также усложняет проблему информационной безопасности – требуется взаимодействие специалистов из разных областей.

В качестве основного инструмента борьбы со сложностью предлагается объектно-ориентированный подход. Инкапсуляция, наследование, полиморфизм, выделение граней объектов, варьирование уровня детализации – все это универсальные понятия, знание которых необходимо всем специалистам по информационной безопасности. То разнообразие технологий защиты, предлагаемых на рынке настолько велико, что знать все, пусть даже поверхностно, не под силу даже самым опытным ИТ-менеджерам. Для правильного выбора небесполезно иметь представление, какие из них могут вовсе не понадобиться. ИТ-менеджеры должны стараться заглянуть как можно дальше вперед, когда речь заходит о внедрении систем, и прежде всего добиваться их корректной работы, а не тратить время и деньги на исправление ошибок.

В заключении можно обобщить: программное обеспечение не должно иметь изъянов, и задача ИТ-менеджеров – стимулировать производителей к выпуску надежных программ, иначе расходы на защиту будут расти. Предприятия должны требовать подтверждения, что программы, которые они покупают, защищены, и производитель проанализировал код с учетом требований безопасности.

Список использованных источников:

1. Мер обеспечения информационной безопасности [Электронный ресурс] Режим доступа: https://cisoclub.ru/mery-obespecheniya-informaczionnoj-bezopasno. Дата доступа 05.04.2022.