An instrument of automation of learning the basics of programming is proposed, which is a system of visual programming embedded into a distance learning environment. The system serves the purpose of improving public availability of visual, interactive learning of programming.

Keywords: flowchart editor, flowchart interpreter, Moodle, Web, JavaScript, TypeScript.

Получено 14.05.2014

УДК 336.7: 004.7.056.53

А. Л. Ахтулов, доктор технических наук, профессор, Тобольский индустриальный институт (филиал) Тюменского государственного нефтегазового университета
Л. Н. Ахтулова, кандидат технических наук, доцент, докторант, Омский государственный университет путей сообщения

ЗНАЧЕНИЕ СТАНДАРТОВ БЕЗОПАСНОСТИ В ОБЕСПЕЧЕНИИ КАЧЕСТВА БАНКОВСКИХ УСЛУГ

Проведен анализ стандартов безопасности в обеспечении информационной безопасности и качества банковских услуг. На основе единого подхода рассматриваются все стороны информационной безопасности банков: системная методология информационной безопасности, эволюция автоматизации банковской деятельности, методы и средства защиты информации в автоматизированных банковских системах.

Ключевые слова: стандарт безопасности, автоматизация деятельности, банковская система, информационная безопасность, защита информации, качество банковских услуг.

На современном этапе развития информационных технологий становится очевидным, что для создания надежных и эффективно работающих банковских систем существует необходимость в обеспечении высокого уровня их информационной безопасности (ИБ). Для этого должны быть точно оценены риски, внедрены необходимые системы защиты. Расширение спектра и рост объемов банковских услуг требует наличие единых подходов, единой терминологии и единых критериев оценки состояния информационной безопасности банков, реализованных на уровне национальных стандартов [1–4], которые отражают мировую практику (COBIT, BS 7799 ISO 17799) банковского сектора: только в этих условиях возможно обеспечение необходимого уровня устойчивой работы банковской системы.

Кроме того, в настоящее время существует отраслевой комплекс стандартов банка России, состоящий из 8 документов [5–12].

Такими образом, в соответствии с международными и национальными стандартами [1–12] обеспечение информационной безопасности в любой деятельности предполагает следующее. Во-первых, определение целей обеспечения информационной безопасности компьютерных систем; во-вторых, создание эффективной системы управления информационной безопасностью; в-третьих, расчет совокупности детализированных показателей для оценки соответствия информационной безопасности заявленным целям; в-четвертых, применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния; в-пятых, использование методик управления безопасностью с обоснованной системой метрик и мер обеспечения информационной безопасности, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью организации.

Критерии оценки безопасности информационных технологий состоят из трех частей. Первая часть [1] определяет концепцию всего стандарта, вторая [2] формализует методы и требования к информационной безопасности. Третья часть [3] полностью посвящена процессам обеспечения доверия (качества) компонентов информационной безопасности, реализующих функции их безопасности. По существу рассматривается регламентирование технологии и процессов обеспечения жизненного цикла программных средств, создаваемых для обеспечения безопасности функционирования и применения систем. При этом акцент документа сосредоточен на информационной безопасности сложных информационных систем, а термин «доверие» применяется как понятие качества или уверенности выполнения требования безопасности.

Нарушения безопасности информационных систем возникают вследствие преднамеренного использования или случайной активизации уязвимостей при их применении, возникающих вследствие следующих недостатков:

– требований, так как информационная система может обладать требуемыми от нее функциями и свойствами, но все же содержать уязвимости, которые делают ее непригодной или неэффективной в части безопасности применения;

– проектирования, так как информационная система не отвечает спецификации, и/или уязвимости являются следствием некачественных стандартов проектирования или неправильных проектных решений;

– эксплуатации, так как информационная система разработана в полном соответствии с корректными

спецификациями, но уязвимости возникают как результат неадекватного управления при эксплуатации.

То есть каждый элемент представляет собой требование для выполнения. Формулировки этих требований к информационной системе (ИС) должны быть четкими, краткими и однозначными. Структура процессов жизненного цикла информационной системы, обеспечивающих информационную безопасность применения в соответствии с классами и стандартами, представлена в таблице.

В зависимости от сложности и критичности требований к безопасности функционирования ИС и доступных ресурсов для ее реализации, стандартом [4] рекомендуется выбирать набор классов, достаточных для обеспечения необходимого качества информационной безопасности ИС – так называемый оценочный уровень доверия. Оценочные уровни доверия образуют возрастающую шкалу достигаемого качества безопасности, которая позволяет соотнести получаемый уровень качества с трудоемкостью его реализации и возможностью достижения этой степени доверия.

Оценочный уровень доверия 1 предусматривает функциональное тестирование и применим, когда требуется некоторая уверенность в правильном функционировании ИС, а угрозы безопасности не рассматривают как серьезные.

Оценочный уровень доверия 2 включает структурное тестирование, содержит требование сотрудничества с разработчиком для получения информации об ИС и результатах тестирования. Такая ситуация может возникать при обеспечении безопасности разработанных ранее систем. Этот уровень требует тестирования и анализа уязвимостей разработчиком, основанного на более детализированных спецификациях.

Структура процессов жизненного цикла информационной системы

Класс	Функции	Содержание
Управление конфигурацией ИС	Автоматизация управления конфигурацией. Возможности управления конфигурацией. Область управления конфигурацией	Обеспечивает сохранение целостности объектов, устанавливая и контролируя определенный порядок процессов корректировки, модификации и предоставления связанной с ними информации
Разработка ИС	Функциональная спецификация ИС. Проект верхнего уровня ИС. Представление реализации ИС. Внутренняя структура функциональной безопасности объекта. Проект нижнего уровня ИС. Соответствие представлений. Моделирование политики ИБ	Определяет требования для пошагового уточнения ИБ, начиная с краткой спецификации объекта в задании и вплоть до фактической реализации
Поставка и эксплуатация ИС	Поставка программного продукта Установка, генерация и запуск ИС	Определяет требования к мерам, процедурам и стандартам, применяемым для безопасной поставки, установки и эксплуатации ИС, чтобы безопасность объектов не нарушалась во время его распространения, внедрения и эксплуатации
Руководства по безопасности ИС	Руководство администратора. Руководство пользователя	Определяет требования, направленные на обеспечение понятности, достаточности и законченности эксплуатационной документации, представляемой разработчиком
Поддержка жизненного цикла безопасности ИС	Безопасность разработки ИС. Устранение дефектов. Определение жизненного цикла ИС. Инструментальные средства и методы	определяет требования для реализации всех этапов разработки четко определенной модели, включая процедуры устранения недостатков и дефектов, правильное использование ИС, а также меры безопасности для защиты среды разработки.
Тестирование ИС	Покрытие тестами ИС. Глубина тестирования ИС. Функциональное тестирование ИС. Независимое тестирование ИС	устанавливает требования, которые должны демонстрировать, что реализованные функции удовлетворяют функциональным требованиям безопасности системы.
Оценка уязвимостей ИС	Анализ скрытых каналов. Неправильное применение ИС. Стойкость функций безопасности объекта. Анализ уязвимостей объекта	определяет требования, направленные на идентификацию уязвимостей, которые могут проявиться и быть активизированы.

Оценочный уровень доверия 3 предусматривает методическое тестирование и проверку, позволяет разработчику достичь доверия путем применения проектирования безопасности без значительного изменения существующей технологии качественной разработки всей системы. Этот уровень представляет значимое увеличение доверия, требуя более полного покрытия тестированием функций и процедур безопасности.

Оценочный уровень доверия 4 предусматривает методическое проектирование, тестирование и углубленную проверку, что позволяет разработчику достичь максимального качества, основанного на регламентированной технологии разработки, которая

не требует глубоких специальных знаний, навыков и других ресурсов. Анализ поддержан независимым тестированием, свидетельством разработчика об испытаниях, подтверждением результатов тестирования разработчиком и независимым анализом уязвимостей.

Оценочный уровень доверия 5 позволяет разработчику достичь максимального качества путем систематического проектирования безопасности, основанного на строгой технологии разработки, поддержанной умеренным применением узко специализированных методов, не влекущих излишних затрат на методы проектирования безопасности. Доверие достигается применением формальной модели политики безопасности.

Оценочный уровень доверия 6 позволяет разработчикам достичь высокой безопасности путем полуформальной верификации всего проекта и тестирования, применением специальных методов проектирования безопасности в строго контролируемой среде разработки с целью получения высокой безопасности системы и защиты активов от значительных рисков, где ценность защищаемых активов оправдывает дополнительные затраты.

Оценочный уровень доверия 7 применим при разработке безопасных систем для использования в ситуациях чрезвычайно высокого риска и/или там, где высокая ценность активов или систем оправдывает максимальные затраты на их безопасность. Этот уровень представляет значительное увеличение доверия, требует всестороннего анализа, использующего формальные представления и формальное соответствие, а также всестороннее независимое тестирование.

Таким образом, функционирование ИС осуществляется следующим образом (рисунок): данные, введенные с рабочих мест пользователей и поступившие на почтовый сервер, направляются на сервер корпоративной обработки данных. Затем данные поступают на рабочие места группы оперативного реагирования и резерва и там принимаются соответствующие решения.

Схема функционирования информационной системы

Действующая в стране нормативная база, которой руководствуются кредитные организации, не адаптирована к особенностям кредитно-финансовой сферы, к тем угрозам, которые в ней присутствуют. Фактически она охватывает только технические стороны вопроса защиты информации. Что же касается управления, аудита и оценки ИБ, то эти аспекты в документах вообще не рассматриваются. Более того, развивается эта база все в том же направлении – в русле совершенствования и усиления требований по технической защите информации и по-прежнему не учитывает реальные модели нарушителя и модели угроз, которые свойственны для кредитно-финансовой сферы.

Информационное противоборство – растянутый во времени процесс, основывающийся на знаниях как собственника, так и злоумышленника, направленный на получение материальной выгоды через контроль над целями своего противника и основанный на избирательных информационных воздействиях, которые позиционированы по пространству и времени.

При этом злоумышленник, как правило, изучает объект нападения и таким образом отрабатывает наиболее эффективный способ реализации собственной цели, выбирая соответствующий метод нападения. Поэтому собственник должен стремиться к выявлению следов такой активности, для чего создает уполномоченный орган – службу ИБ (подразделение или лицо, ответственные за обеспечение ИБ в организации).

Философия информационного противоборства исходит из того, что изначально знания собственника относительно его потенциального противника (или злоумышленника) минимальны, как, впрочем, и злоумышленника относительно слабых мест информационных активов собственника. Поэтому собственник (его служба ИБ) строит предположения, гипотезы

относительно потенциального противника, которые затем нуждаются в подтверждении, в том числе и в рамках практической деятельности служб ИБ. Главным инструментом собственника является основанный в первую очередь на его опыте прогноз (разработка модели угроз и модели нарушителя) относительно его информационных активов. И чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ в организации при минимальных ресурсных затратах. Таким образом, наиболее правильный и эффективный способ добиться минимизации рисков нарушения ИБ для собственника – это разработать на основе точного прогноза политику ИБ и в соответствии с ней построить систему управления ИБ в организации. Требования по разработке политики ИБ организации составляют значительную часть требований стандарта, ибо именно положения этой политики определяют цели и задачи по обеспечению ИБ, права, обязанности и ответственность службы ИБ.

В стандарт включены требования ИБ по семи областям, которые обязательно должны найти отражение в политике ИБ организации. Разделы стандарта по модели зрелости процессов управления ИБ организации, а также ее аудиту и мониторингу основываются на соответствующих общепризнанных в международном сообществе подходах, изложенных, в таких стандартах, как COBIT и BS 7799-2, а также других документах.

Важным вопросом является также использование результатов оценки кредитной организации [13, 14]. Мировая практика показывает, что результатом оценки может быть сертификат соответствия, рейтинг организации в рамках профессионального сообщества и т. п. Как сертификат, так и рейтинг организации – это информация для пользователей, потребителей продукции и услуг организации, поэтому она должна быть публичной. Как представляется, не каждая российская кредитная организация готова к тому, чтобы информация об уровне ее ИБ была публично доступной. Однако это требование времени и международного сообщества, и, как можно прогнозировать, в самом ближайшем будущем будет и требованием клиентов банков. Значит, к этому необходимо стремиться, что наверняка успешно скажется и на бизнесе кредитной организации.

Банк России намерен вести работы в этом направлении и дальше. К этому основному документу планируется разработать тематические приложения, которые позволят сделать так, чтобы деятельность внутреннего контроля коррелировалась с теми стандартами, которые приняты в международной практике [8], в результате чего банк получит возможность сам себя регулярно контролировать, что зачастую значительно выгоднее, чем приглашать внешнего аудитора.

Выполнение организациями требований стандартов значительно минимизируют риски информационных технологий. Банк России, разработав национальный стандарт информационной безопасности для применения в кредитно-финансовой сфере, способствовал повышению стабильности функционирования банковской системы Российской Федерации.

В заключение следует отметить, что в настоящее время стандарты информационной безопасности Банка России широко используются в кредитных организациях, целью которого является создание национальной платежной системы Российской Федерации.

Библиографические ссылки

1. ГОСТ Р ИСО/МЭК 15408-1–2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Ч. 1. Введение и общая модель. – М. : Стандартинформ, 2009. – 40 с.

2. ГОСТ Р ИСО/МЭК 15408-2–2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Ч. 2. Функциональные требования безопасности. – М. : Стандартинформ, 2009. – 174 с.

3. ГОСТ Р ИСО/МЭК 15408-3–2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Ч. 3. Требования доверия к безопасности. – М. : Стандартинформ, 2009. – 112 с.

4. ГОСТ Р ИСО/МЭК 17799–2005. Информационная технология. Практические правила управления информационной безопасностью. – М. : Стандартинформ, 2006. – 61 с.

5. СТО БР ИББС 1.0–2010. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. – М., 2010. – 42 с.

6. СТО БР ИББС-1.2–2010. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-20xx. – М., 2010. – 74 с.

7. РС БР ИББС-2.1–2007. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0. – М., 2007. – 15 с.

8. СТО БР ИББС-1.1–2007. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности. – М., 2007. – 14 с.

9. РС БР ИББС-2.0–2007. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями стандарта СТО БР ИББС-1.0. – М., 2007. – 14 с.

10. РС БР ИББС-2.2–2009. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков информационной безопасности. – М., 2009. – 23 с.

11. РС БР ИББС-2.3–2010. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации. – М., 2010. – 18 с.

12. РС БР ИББС-2.4–2010. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации. – М., 2010. – 11 с.

13. *Ахтулов А. Л.*, *Бирюкова Е. Ю.* Система менеджмента качества как основа конкурентоспособности коммерческого банка // Вестник ИжГТУ. – 2009. – № 4(44). – С. 78–79.

14. Измерение результативности системы менеджмента качества как инструмент совершенствования деятельности организации / А. Л. Ахтулов, Л. Н. Ахтулова, А. Ю. Мустакова, С. Т. Ташмагамбетова // Омский научный вестник. – 2013. – № 1(117). – С. 132–136.

A. L. Akhtulov, DSc in Engineering, Professor, Tobolsk Industrial Institute SEU HPF "The Tyumen State Oil and Gas University" (Branch of TyumSOGU)
L. N. Akhtulova, PhD in Engineering, Associate Professor, DSc Applicant, Omsk State University of Means of Communication

Value of Safety Standards in Maintenance of Bank Services Quality

The analysis of safety standards in maintenance of information safety and quality of bank services is carried out in the paper. On the basis of the uniform approach the parties of information safety of banks are considered altogether: system methodology of information safety, evolution of automation of bank activity, methods and means of protection of the information in automated bank systems.

Keywords: standard of safety, automation of activity, bank system, information safety, protection of information, quality of bank services.

Получено 02.06.2014

УДК 004.934.2

С. В. Моченов, кандидат технических наук, Ижевский государственный технический университет имени М. Т. Калашникова
М. А. Шаронов, аспирант, Ижевский государственный технический университет имени М. Т. Калашникова
Р. Р. Ахметгалеев, магистрант, Ижевский государственный технический университет имени М. Т. Калашникова
Д. В. Бортник, магистрант, Ижевский государственный технический университет имени М. Т. Калашникова

ПРИМЕНЕНИЕ БЫСТРОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ ДЛЯ ВЫДЕЛЕНИЯ ЯЗЫКОВЫХ ОБЪЕКТОВ РЕЧЕВОГО СИГНАЛА

Рассматриваются вопросы разделения речевого участка на отдельные сегменты с целью выделения наиболее информативных частей, связанных с определенным звуком и соответствующей ему фонемой. В процессе дихотомического деления фрагмента речи и выявления на основе спектрального анализа зон стабилизации осуществляется выделение языковых объектов и определение порядка их следования в речевой цепочке.

Ключевые слова: сегмент речи, языковой объект, различительные признаки звуков, спектральный анализ, процесс дихотомического деления, зона стабилизации звука, фонема.

В настоящее время большое внимание уделяется развитию интеллектуальных информационных систем с возможностями организации диалога «пользователь – система» на естественном языке. Построение подобных систем основано на разработке специальных алгоритмов анализа и синтеза речи. Сложность процедуры автоматического анализа речевых сигналов, качество анализа связаны с необходимостью учета большого количества факторов, определяемых: динамикой речи; индивидуальными акустическими параметрами диктора; сложностью выявления полезных различительных признаков, используемых для выделения и распознавания отдельных фонем, слов, законченных речевых фраз; сложностью алгоритмов анализа и синтеза смыслообразующих компонент языковых объектов [1] и др.

Основная работа исследователя по анализу речевых сигналов, как правило, связана с поиском вариантов извлечения полезной информации, неравномерно распределенной во времени и зависящей от звукового состава анализируемого фрагмента речи.

Один из вариантов решения задачи автоматического распознавания речи предполагает разбиение речевого фрагмента на дискретные единицы, отдельные сегменты речевого потока, связанные с отдельным звуком. Однако такое направленное сегментирование сложно осуществить на практике [2].

В данной работе вопросы распознавания отдельных фонем или слов затрагиваются лишь частично. Основное внимание уделено решению задачи однозначного разделения речевого участка на отдельные сегменты с целью выделения наиболее информативных частей, связанных с определенным звуком и соответствующей ему фонемой.

Для работы в реальном масштабе времени и для получения амплитудно-частотного спектра сигнала удобно использовать быстрое преобразование Фурье