Реалізація загроз здійснюється зловмисниками через використання вразливостей ІС банку.

Процес ідентифікації вразливостейІС слід здійснювати у наступних областях:

− інформаційна система у цілому;

− фізичне середовище;

− характеристика та конфігурація програмно-технічних засобів, програмного забезпечення,технологічного та телекомунікаційного обладнання;

− характеристика системи управління інформаційною безпекою (СУІБ);

− характеристика персоналу ІС та служби захисту інформації (СЗІ);

− характеристика постачальників програмного забезпечення та апаратних засобів ІС;

− характеристика організації, що надає послуги з аудиту ІБ інформаційної системи банку.

Для виявлення вразливостей в залежності від вимог до захисту інформації та бізнес-процесу/банківського продукту, а також від застосованої інформаційно-телекомунікаційної технологіїслід застосовувати різні методи аналізу захищеності ІС [3]. До них належать:

− спеціальні програмні засоби сканування вразливостей;

− засоби тестування та поточної оцінки інформаційної безпеки;

− тести на проникнення;

− перегляд коду програмно-технічних комплексів;

− аналіз відомих та виявлених вразливостей та порушень ІБ, що досліджені та систематизовані СЗІ банків;

− моніторинг процесів ІС та дій її персоналу.

Перелічені методи не тільки дають змогуідентифікувати вразливості, але й ліквідувати певну загрозу.

ЛІТЕРАТУРА

1. SO/IEC 27005 «Information technology – Security techniques – Information security risk management» (Управління ризиками інформаційної безпеки).

2. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України.

3. Сізова Н. Д., Здановський Я. В. Захист інформації в банківських та комерційних системах : навчальний посібник. – Х. : ХДТУБА, 2009. – 112 с.

К. Чоговадзе,
К. Чоговадзе, студентка 5 курса
факультета Компьютерных наук и инновационных технологий;
Международный гуманитарный университет

РАЗРАБОТКА АРХИТЕКТУРНОЙ МОДЕЛИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

Обеспечение безопасности компьютерных систем (КС) в наши дни становится все более актуальным в связи с постоянным развитием информационных технологий и появлением новых способов хищения, искажения информации, нарушения работоспособности КС. При этом штатное функционирование государственных и коммерческих КС становится невозможным без постоянного поддержания их конфиденциальности и целостности.

Наряду с развитием информационных технологий растут и требования к поддержанию безопасности. Одновременно статистика свидетельствует о росте количества инцидентов, основными причинами которых являются недостатки в разработке и эксплуатации средств защиты. Эта проблема особенно остро стоит в критических КС: в системах управления производством, движением, финансовыми операциями, обработки категорированной информации [1].

При разработке архитектурной модели обеспечения безопасности большое внимание должно уделяться построению архитектуры и разработке прототипа системы, реализующей предложенную методику автоматизации настройки безопасности КС, разработке методики автоматизированной настройки КС с соблюдением заданных требований по безопасности и показателей эффективности на основе решения оптимизационной задачи [2; 3].

В данной работе предлагается вариант архитектуры системы, реализующей предложенную методику автоматизации настройки безопасности КС, и представлены опытные результаты работы прототипа системы. В основе разработанной системы, изображенной на рисунке 1, лежит логический процессор, который на основании правил ПБ, профиля КС и описания текущих ресурсов ОС согласно имитационной модели подсистемы контроля доступа КС генерирует множество конфигурационных параметров защиты ОС. Концептуальные принципы работы логического процессора представлены на рисунке 2.

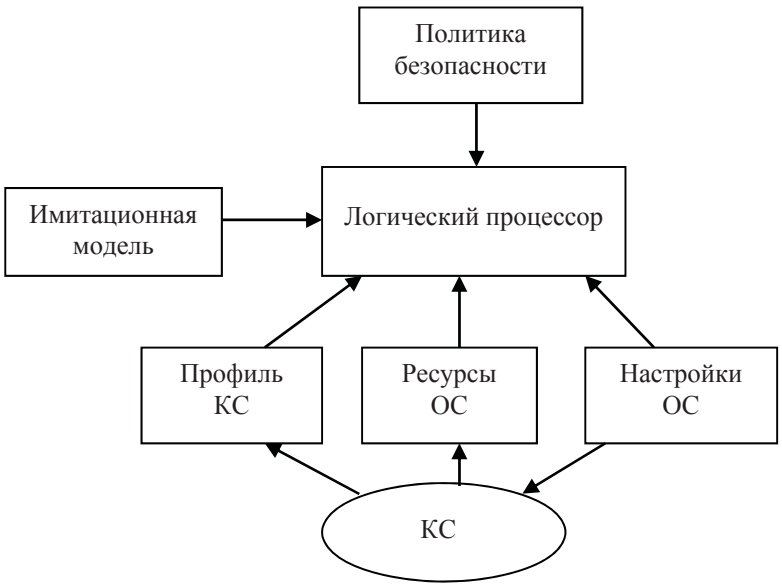

Рисунок 1. Архитектура системы настройки безопасности ОС

Применение предложенного подхода к построению множества конфигурационных параметров защиты ОС позволяет автоматизировать процесс настройки безопасности КС согласно действующей ПБ и с учетом устойчивости безопасного состояния [4–6].

Эффективность предложенного подхода и архитектуры системы автоматизированной настройки безопасности КС подтверждается полученными экспериментальными результатами. Тестирование выполнялось в корпоративной сети из 118 компьютеров, среди которых два файловых сервера, один Web/Mail сервер и 115 рабочих станций.

Полученные экспериментальные результаты приведены в таблице 1.

Рисунок 2. Работа логического процессора

Таблица 1.

Результаты применения системы автоматизированной настройки безопасности КС

Характеристика	Настройка безопасности		
	Разработанная система	MS Baseline Security Analizer	«Ручная«настройка
Время, затраченное на выполнение настройки безопасности	2.5 часа	1 день	1 неделя
Количество ошибок (несоответствий критериям безопасности)	0	5	11
Успешность проведения атак	2 из 50	24 из 50	18 из 50
Время до первой корректировки настройки безопасности	28 дней	2 дня	5 дней

В работе получены следующие основные результаты: разработан алгоритм автоматизированной настройки безопасности КС, а также разработаны архитектура и прототип системы, реализующей предложенную методику автоматизации настройки безопасности КС.

ЛИТЕРАТУРА

1. Ленков С. В. Методы и средства защиты информации : в 2-х томах / Ленков С. В., Перегудов Д. А., Хорошко В. А. – К. : Арий, 2008.

2. Горелик В. А. Исследование операций / Горелик В. А., Ушаков И. А. – М. : Машиностроение, 1986. – 288 с.

3. Вунш Г. Теория систем / Вунш Г. – М. : Сов. радио, 1978. – 288 с.

4. Информационно-коммуникационные технологии в образовании [Электронный ресурс]. – Режим доступа: http://www. ict. edu. ru/ft/002443/chapter1. pdf

5. Будзко В. И. Современные подходы к обеспечению катастрофоустойчивости информационно-телекоммуникационных систем высокой доступности / В. И. Будзко, П. А. Кейер, М. Ю. Сенаторов // Наукоемкие технологии. – 2008. Т. 9. – № 5. – С. 14–24.

6. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и Техника, 2004. – 384 с.