УДК 004.056.53

О.С. АНДРЕЄВ, М.В. ЛЮТА, М.В. ЗАХАРОВА

Київський національний університет технологій та дизайну

АНАЛІЗ ТА ОЦІНКА ЗАГРОЗ НА ІНФОРМАЦІЙНІ РЕСУРСИ КОМП‘ЮТЕРНИХ СИСТЕМ, ЯКІ ПРАЦЮЮТЬ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Робота присвячується аналізу загроз на інформаційні ресурив банкоматів і платіжних терміналів та класифікації цих загроз для подальшого її використання в системі аудиту інформаційних ресурсів.

Ключові слова: *класифікація загроз, інформаційні ресурси, банкомати, безпека.*

Велика кількість електронних злочинів пов’язана із несанкціонаваним доступом до інформаційних ресурсів комп’ютерних систем, які працюють в режимі реального часу. Такі системи керують банкоматами та платіжними терміналами, їх власники змушені звертатися до експертів, які проводять аудиторську перевірку захищеності інформаційних ресурсів комп‘ютерної системи. Чітка система класифікації загроз допоможе експерту розробити ефективні рекомендації по підвищенню рівня захищеності інформаційних ресурсів.

Протягом останніх 10 років спостерігається збільшення кількості банкоматів у світі – до 2,4 млн. В Україні, на даний момент, уведено в експлуатацію 37 тис. банкоматів. З ростом числа банкоматів збільшилася і кількість злочинів, пов‘язаних із ними. Значну частку таких злочинів становить несанкціонований доступ до інформаційних ресурсів (ІР) комп‘ютерної системи (КС), яка керує банкоматом.

Метою захисту інформації є збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, оброблення, зберігання, пошуку та надання користувачам. Ці технології мають ураховувати особливості інформації, які й роблять її цінною, а також давати змогу користувачам різних категорій працювати з інформаційними ресурсами (створювати, знаходити, копіювати, узагальнювати, порівнювати, модифікувати, перетворювати, знищувати тощо).

Комп'ютерні системи, що працюють в режимі реального часу – це комп'ютерні системи, які дозволяють користувачам мати доступ до даних і програм безпосередньо через термінал. Такі системи можуть складатися з універсальних обчислювальних машин, мінікомп’ютерів або персональних комп'ютерів, з’єднаних в мережу. Коли господарюючий суб'єкт використовує комп'ютерну систему, що працює в режимі реального часу, використовувані технології можуть бути досить складними і можуть мати зв'язок зі стратегічними бізнес-планами господарюючого суб'єкта [1].

Кількість банкоматів в Україні за останній рік збільшилась всього на 4 тис. Але все ще залишається 79% незахищених банкоматів.

Несанкціонований доступ до ІР КС банкомату завдає значних збитків. З метою запобігання несанкціонованого доступу до ІР КС, необхідно провести аудит інформаційної безпеки. Аудит проводиться експертом, який збирає, аналізує дані та розробляє рекомендації щодо підвищення рівня захищеності ІР КС. Для того, щоб експерту розробити максимально ефективні рекомендації по підвищенню рівня захищеності ІР КС, необхідно виявити всі можливі загрози.

Аналіз стандартів для проведення аудиту показав, що всі вони містять лише загальні рекомендації, які повинен виконати експерт при проведенні аудиту ІР КС [2, 3].

Таким чином, при використанні сучасної методичної бази, оцінка ефективності засобів захисту інформації носить нечіткий, суб'єктивний характер [4]; практично повністю відсутні нормовані кількісні показники, що враховують можливі випадкові або навмисні дії. У результаті досить складно, а часто і неможливо, оцінити якість функціонування комп'ютерної системи за наявності несанкціонованих впливів на її елементи, а, відповідно, і визначити, який варіант проектованої системи краще.

Для розробки ефективних рекомендацій по підвищенню рівня захищеності ІР КС потрібно точно класифікувати та оцінити загрози.

Тому, основною задачею даної роботи є аналіз і оцінка загроз ІР КС, що дозволить підвищити рівня захищеності ІР КС та знизити ризик втрати ІР.

Ризик виникнення помилок у системах, що працюють в режимі реального часу, може збільшитися в результаті наступних факторів [1]:

– Термінали, що працюють в режимі реального часу, можуть забезпечити можливість несанкціонованого використання за допомогою:

– зміни раніше введених операцій і залишків по рахунках;

– зміни комп'ютерних програм;

– доступу до інформації та програмами на відстані.

– Якщо обробка в режимі реального часу переривається з якої-небудь причини, існує ймовірність втрати операцій і файлів, а також того, що відновлена інформація не може бути точною і повною.

– Доступ в режимі реального часу до інформації та програмам через телекомунікації може забезпечити можливість несанкціонованого доступу.

Загрози інформаційної безпеки класифікуються за кількома ознаками:

1) за складовими інформаційної безпеки (доступність, цілісність, конфіденційність) спрямовані загрози;

2) по компонентах інформаційних систем, на які загрози націлені (дані, програми, апаратура);

3) за характером впливу (випадкові або навмисні, дії природного або техногенного характеру);

4) по розташуванню джерела загроз (всередині або поза розглянутої інформаційної системи).

При аналізі загроз інформаційної безпеки відправною точкою є визначення складової інформаційної безпеки, яка може бути порушена тією чи іншою загрозою: конфіденційність, цілісність або доступність.

При аналізі загроз за характером впливу, виявлено що інформація піддається різним випадковим впливам на всіх етапах циклу життя системи.

Причинами випадкових впливів при експлуатації можуть бути:

1) аварійні ситуації через стихійних лих і відключень електроживлення (природні та техногенні впливи);

2) відмови і збої апаратури;

3) помилки в програмному забезпеченні;

4) помилки в роботі персоналу;

5) перешкоди в лініях зв'язку через впливів зовнішнього середовища.

Загрози, що класифікуються за розташуванням джерела загроз, бувають внутрішні і зовнішні.

Зовнішні загрози обумовлені застосуванням обчислювальних мереж і створення на їх основі інформаційних систем.

Особливість обчислювальної мережі полягає в тому, що її компоненти розподілені в просторі. Зв'язок між вузлами мережі здійснюється фізично за допомогою мережевих ліній і програмно за допомогою механізму повідомлень. Керуючі повідомлення і дані, що пересилаються між вузлами мережі, передаються у вигляді пакетів обміну. Особливість даного виду загроз полягає в тому, що місце розташування зловмисника спочатку невідомо.

Існує декілька можливих способів здійснення загрози:

1) технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні та радіотехнічні, хімічні канали;

2) каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

3) несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації, застосування закладних пристроїв чи програм та розповсюдження комп’ютерних вірусів.

Підключення до КС відбувається по каналам зв‘язку між банкоматом та авторизованим центром. Підключення по каналам зв‘язку дає змогу перехоплювати транзакції.

Виділяють три основних типи загроз з транзакціями: модифікація даних, викрадення, а також порушення доступності відправки транзакції. Виділяють кілька типів модифікації: коригування суми операції для зміни даних про запит виданих грошових коштів; коригування ідентифікаторів платіжного інструменту - номера картки; корегування призначення платежу при операціях card-to-card або person-to-person через банкомати (цілісність даних одержувача у складі транзакції не контролюється, така підміна може бути здійснена за відсутності шифрування транзакції).

Особливий тип отримання інформації технічними каналами при операціях з картками – скіммінг. Скіммінг представляє собою крадіжку даних з карти за допомогою спеціального пристрою, що зчитує. Зловмисники копіюють всю інформацію з магнітної смуги карти (ім'я власника, номер картки, термін закінчення терміну її дії, CVV-і CVC-код). Оскільки скіммінг-пристрої дуже складні і їх часто важко виявити багато карт опиняються під загрозою [5]. Вразливим місцем КС також є порти та операційна система.

При аналізі небезпечних загроз та моделюванні їх впливу на ІР КС, в якості вхідних даних враховуються тип та цілі зловмисника, засоби реалізації загрози, тощо. Далі аналізуються дестабілізуючі дії по кожному об’єкту для кожного зловмисника. Із всіх можливих дій формується множина всіх можливих загроз ІБ={X}(див рис.1).

Рис. 1. **Проведення аналізу небезпечних загроз та моделюванні їх дії на ІР КС**

Моделювання та класифікацію джерел загроз проводять на основі аналізу взаємодії логічного ланцюжка:

джерело загрози – вразливість системи – атака

Після аналізу виявлених вразливостей інформаційної безпеки, сформовано перелік загроз інформаційної безпеки для АТМ:

1. Крадіжка носіїв інформації та відмови носіїв даних;
2. Відмова програмного забезпечення;
3. Віруси, їх впровадження в ПЗ;
4. Ненавмисне видалення інформації;
5. Крадіжка аутентифікаційних даних користувача();
6. Крадіжка відпрацьованих матеріалів;
7. Зловживання повноваженнями;
8. Загрози, що реалізуються безконтактним способом (збір електромагнітних випромінювань, перехоплення сигналів, що наводяться в ланцюгах, візуально-оптичні способи видобутку інформації);
9. Ненавмисні помилки користувачів, системного адміністратора та інших осіб, які обслуговують АТМ.

У ході аналізу необхідно переконатися, що всі можливі джерела загроз ідентифіковані і зіставлені з джерелами загроз всі можливі уразливості.

На підставі результатів, отриманих в ході обстеження ІР КС, оцінки загроз, вразливостей і ризиків розробляються рекомендації з удосконалення захисту інформації до необхідного рівня.

Висновки

Таким чином, проведення аналізу та оцінки загроз безпеки дозволить підвищити рівень захищеності інформаційних ресурсів комп‘ютерних систем, які працюють в режимі реального часу. Приведена класифікація небезпечних загроз на інформаційні ресурси, визначення вразливих місць КС дозволить вибрати найбільш економічні та ефективні засоби захисту та надати своєчасні рекомендації по забезпеченню безпеки.

Список використаної літератури

1. ПАП 1002 «Аудит в среде информационных компьютерных систем - компьютерные системы, работающие в режиме реального времени».
2. ГСТУ СУІБ 1.0/ISO/IES 27001:2010 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги» (ISO/IEC 27001:2010, MOD).
3. ГСТУ СУІБ 2.0/ISO/IES 27002:2010 «Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою» (ISO/IEC 27002:2010, MOD).
4. Л. Хмелев. Оценка эффективности мер безопасности, закладываемых при проектировании электронно-информационных систем. Труды научно-технической конференции «Безопасность информационных технологий», Пенза, июнь 2001.
5. European Network and Information Security Agency (ENISA), ATM Crime, August, 2009.

Стаття надійшла до редакції / Article received: 01.07.2013

Рецензент: д.т.н., проф. кафедри інформаційних, комп’ютерних технологій КНУТД Рябцев В.Г.

Анализ и оценка угроз на информационные ресурсы компьютерных систем, работающих в режиме реального времени

Андреев А.С., Лютая М.В., Захарова М.В.
Киевский национальный университет технологий и дизайна

Эта работа посвящена анализу угроз информационных ресурсов для банкоматов и платежных терминалов и классификации этих угроз для дальнейшего ее использования в системе аудита информационных ресурсов.

Ключевые слова: классификация угроз, информационные ресурсы, банкоматы, безопасность.

Analysis and assessment of threats to the information resources of the computer systems that operate in real time

Andreev A., Lyuta M., Zakharova M.
Kyiv National University of Technologies and Design

This work is devoted to the analysis of threats to information resources for ATMs, payment terminals and classification of these threats to further its use in auditing information resources.

Keywords: classification of threats, information resources, ATMs, security.

УДК 675.026

О.А. ОХМАТ, О.Р. МОКРОУСОВА

Київський національний університет технологій та дизайну

ВИКОРИСТАННЯ ОКИСЛЕНИХ БІЛКОВИХ СПОЛУК ДЛЯ ФАРБУВАННЯ ВОРСОВИХ ШКІР

У статті розглянуті результати дослідження впливу різних факторів на процес фарбування аніонними барвниками. Визначено властивості ворсових шкір після фарбування при різних умовах. Установлено оптимальні параметри процесу фарбування, при яких досягаються найкращі якісні характеристики пофарбованого велюру.

Ключові слова: *фарбування, аніонний барвник, окислені білкові сполуки, ворсові шкіри, інтенсивність, рівномірність, якість забарвлення.*

Підвищення рівня якості за рахунок збільшення стійкості забарвлення натуральної шкіри до різних физико-хімічних дій є однією з основних задач технології шкіри. Вимоги до стійкості забарвлення, залежно від вигляду і призначення шкіри, змінюються в досить широких межах. Наприклад, для одягових і галантерейних шкір, що багато разів піддаються в процесі експлуатації так званим «мокрим» впливам, важливе значення мають показники стійкості забарвлення до дії води і хімічного чищення; для взуттєвих шкір - стійкості забарвлення до дії поту, води. Особливого значення ці показники набувають для ворсових шкір (велюру), які виробляються або з лицьового, або з бахтармяного спилку шкур великої рогатої худоби. Перерахованих властивостей не можна досягти лише одним хімічним матеріалом, тому для надання ворсовим шкірам широкого спектру властивостей на одному технологічному процесі необхідне застосування комплексу хімічних матеріалів, що включає барвники, підсилювачі кольору, гідрофобізатори, вирівнювачі, зв'язуючі компоненти, в ролі яких можуть застосовуватися похідні колагену.

Досвід промисловості з застосування оксипохідних колагену при фарбуванні шкір аніонними барвниками показав досягнення кращого відпрацювання фарбувального розчину, що дозволяє на 10% знизити витрати барвника, не знижуючи інтенсивність забарвлення [1]. Завдяки наповнювальній здатності продуктів модифікації колагену, їх можна застосовувати в технологіях рідинного оздоблення