Міністерство освіти і науки України
Державна наукова установа "Інститут модернізації змісту освіти"
Центральноукраїнський національний технічний університет

Комп'ютерна інженерія і кібербезпека: досягнення та інновації

Матеріали Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених

(м. Кропивницький, 27–29 листопада 2018 р.)

Кропивницький ЦНТУ 2018

УДК 004
ББК 32.97
К63

К63 **Комп'ютерна інженерія і кібербезпека : досягнення та інновації** : матеріали Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених (м. Кропивницький, 27–29 листоп. 2018 р.) / М–во освіти і науки України, Держ. наук. установа "Інститут модернізації змісту освіти", Центральноукр. нац. техн. ун–т. — Кропивницький: ЦНТУ, 2018. — 448 с.

Збірник містить тези доповідей учасників Всеукраїнської науково-практичної конференції здобувачів вищої освіти та молодих учених "Комп'ютерна інженерія і кібербезпека: досягнення та інновації" (м. Кропивницький, 27–29 листопада 2018 року). Праці присв'ячені актуальним питанням інформаційних систем і технологій, технологій проектування комп'ютерних систем та мереж, інженерії програмного забезпечення, комп'ютерних систем штучного інтелекту, мережних ІТ, комп'ютерної електроніки, логіки, схемотехніки, графіки, нормативно-правових засад забезпечення кібернетичної безпеки, інформаційної безпеки національного сегмента кіберпростору, боротьби з кіберзлочинністю, захисту програм та даних в комп'ютерних системах і мережах.

Видання призначене для аспірантів, докторантів, науковців, викладачів і студентів технічних спеціальностей закладів вищої освіти та всіх, хто цікавиться питаннями комп'ютерної інженерії й кібернетичної безпеки.

УДК 004
ББК 32.97
К63

Рекомендовано до друку Науково-технічною радою Центральноукраїнського національного технічного університету (протокол № 11 від 29 листопада 2018 р.)

Відповідальний за випуск: канд. техн. наук Доренський О. П.

Тексти матеріалів конференції друкуються у авторській редакції, мовою оригіналу. За достовірність наведених у публікаціях даних, назв, імен, цитат та іншої інформації відповідальність несуть автори.

Адреса організаційного комітету конференції
Центральноукраїнський національний технічний університет
Кафедра кібербезпеки та програмного забезпечення
просп. Університетський, 8, м. Кропивницький, 25006
(0522) 55-10-49, 39-04-49; cntu-conference@ukr.net; www.kntu.kr.ua

ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

КОМП'ЮТЕРНА ЕЛЕКТРОНІКА, ЛОГІКА Й СХЕМОТЕХНІКА

КОМП'ЮТЕРНА ГРАФІКА

НОРМАТИВНО–ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ

ЗАХИСТ ПРОГРАМ ТА ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

УДК 004.056

Черняк Т. О., Глушко В. В.
Донецький національний технічний університет

Вдосконалення методів безпечного хешування при забезпеченні автентичності та цілісності даних у автоматизованих банківських системах

Високорентабельна економіка у процесі розвитку потребує впровадження ультрасучасної системи обігу грошей, а також експлуатації ефективних платіжних інструментів. Обсяги даних, які оброблюються у сучасних внутрішніх платіжних системах (ВПС), постійно зростають, з'являються нові електронні послуги, стрімко розвивається обчислювальна техніка – все це потребує збільшення показників безпеки даних у ВПС.

Актуальність теми зумовлена необхідністю створення теоретичної рекомендації по використанню методів ключового хешування, що забезпечують цілісність та автентичність інформації у всесвітніх платіжних системах комерційних банків. Нажаль, зараз не існує механізмів та концепцій, які б гарантували фінансову безпеку національної платіжної системи в цілому та банківської діяльності окремо, щоб при цьому ще були науково обґрунтовані.

Постійний розвиток ринкової економіки потребує належної платіжної системи, яка дозволить проводити розрахунки, що виповідатимуть світовим загальноприйнятим стандартам: де на першому находяться безпека, надійність та час проведення платежів. Національна платіжна система є складною та багаторівневою системою із централізованим керуванням. Саме це забезпечує надійний і важливий у стратегічному плані канал, через який фінансові транзакції проводяться.

НПС – це багаторівнева складна система управління критичного застосування або СУКЗ, де передача даних потребує постійного контролю над безпекою, при цьому це повинно здійснюватися на кожному рівні обов'язково. Підсистема криптографічної безпеки даних – це одна з найважливіших частин у складі ВПС, реалізація базується на відповідних механізмах та протоколах.

Питання безпеки ВПС та мереж зв'язку банківської й фінансово-кредитних сфер можна без перебільшення віднести до національного рівня. Методи обробки, зберігання та передачі даних, які використовувалися у інформаційних системах останні роки, самі по собі були факторами появи загроз. Вони пов'язані з ймовірністю повної втрати або спотворення чи втрати конфіденційності інформації, яка направлена чи належить кінцевому користувачеві.

Загроза інформаційної безпеки в інформаційних системах – це можливість втручання у дані, які обробляються автоматизованою системою, що може призвести до копіювання даних чи їх спотворення або знищення, блокування доступу, в тому числі втручання у дію роботу компонентів автоматичної системи.

Класифікація загроз інформаційної безпеки відбувається за наступними критеріями: компоненти інформаційних систем (ІС), на які направлені загрози (програмне забезпечення, дані, інфраструктура та підтримуюче обладнання); мета впливу; зовнішнє чи внутрішнє джерело загрози; спосіб реалізації (техногенний чи природній характер). [1]

Мета впливу загроз ділиться на три основні типи: загроза цілісності, доступності та конфіденційності.

На даний момент оцінка стану інформаційної безпеки вказує на те, що її обсяг та якісні характеристики не відповідають сучасним потребам. Тому визначення основних

реальних та потенційних загроз, що негативно будуть впливати на процес стабільного урегулювання інформаційної безпеки є важливим завданням.

Якщо проаналізувати загальну класифікація загроз інформаційної безпеки на ВПС, то можна зробити висновки, що є джерела ненавмисних загроз ІС:

- поламка складових частин обладнання;
- збій у роботі програмного забезпечення;
- неправильні дії з боку користувачів та персоналу;
- ненавмисні помилки у програмно-апаратному забезпеченні.

Звичайно, такі загрози наносять суттєвий збиток, але навмисні загрози з точки зору функціювання є більш значними, бо сама їх мета – це завдання збитків ІС або її користувачам. Такі загрози реалізуються шляхом довготривалої та масової атаки за допомогою вірусів чи несанкціонованих запитів. Атаки матимуть наступні наслідки: повна чи часткова втрата інформації, підтасовка даних, доступ до інформації отримують сторонні особи. Не важко уявити до чого можуть привести події такого роду. Тому протидія загрозам інформаційної безпеки, які вже були розглянуті вище, є пріоритетною задачею засобів захисту комп'ютерних систем та мереж. Послуги інформаційної виступають в якості засобів захисту ІС.

Рисунок 1 – Види послуг безпеки

За рахунок основних досягнень у сфері ІТ та комунікацій ВПС постійно розвивають да вдосконалюють свої функції. А саме послуги оплати насамперед через банкомати, термінали та віддалених користувачів; продаж товарів через онлайн-магазини тощо.

Характеристики обчислювальної техніки постійно модернізуються, а її продуктивність постійно зростає – це підтверджує закон Мура. Таким чином, інформаційні системи постійно вразливі перед різноманітними атаками та загрозами.

Висновоки. На даний момент оцінка стану інформаційної безпеки вказує на те, що її обсяг та якісні характеристики не відповідають сучасним потребам. Тому визначення основних реальних та потенційних загроз, що негативно будуть впливати на процес стабільного урегулювання інформаційної безпеки є важливим завданням.

Список використаних джерел

1. *Соколов А. В. Защита от компьютерного терроризма. [Текст] / Соколов А. В., О. М. Степанюк. – БХВ-Петербург Арлит, 2002. – 496 с.*
2. *Конеев И. Р. Информационная безопасность предприятия [Текст] / И. Р. Конеев, А. В. Беляев. – БХВ-Петербург, 2003. – 752 с.*

Наукове видання

КОМП'ЮТЕРНА ІНЖЕНЕРІЯ І КІБЕРБЕЗПЕКА: ДОСЯГНЕННЯ ТА ІННОВАЦІЇ

Матеріали Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених

(м. Кропивницький, 27-29 листопада 2018 р.)

Технічний редактор *О. П. Дóренський*

Підписано до друку 29.11.2018. Формат 60x84/8. Папір офсетний.
Надруковано на ризографі. Тираж 245 прим.