6. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto, J. Nechvatal et al. National Institute of Standards and Technology Special Publication, 2010. 131 p.

Ключові слова: криптографія, генератор псевдовипадкових ключових послідовностей, стохастичний тест.
Ключевые слова: криптография, генератор псевдослучайных ключевых последовательностей, стохастический тест.
Key words: cryptography, pseudo-random key sequence generator, stochastic test.

КУХАРЕНКО СЕРГІЙ ВІКТОРОВИЧ

Національний університет «Одеська юридична академія», доцент кафедри кібербезпеки, кандидат технічних наук

ПІДХІД ЩОДО ОБҐРУНТУВАННЯ ВИМОГ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Впровадження сучасних цифрових технологій в різні сфери життя і виробництва та комп'ютеризація повсякденного життя, електронний документообіг, створення великих баз даних, необхідність прийняття відповідальних рішень за короткий час або в критичних ситуаціях, необхідність обробки великих об'ємів інформації тощо потребує створення у кожній без виключення державній установі, комерційних структурах, автоматизованих інформаційно-аналітичних систем управління. Це потребує створення системи захисту інформації та її об'єднання з автоматизованою системою управління (АСУ) в єдину систему та встановлення жорстких логічних та функціональних зв'язків між ними. Як показує практика, саме якість зазначених зв'язків визначає рівень ефективності автоматизованої системи управління з системою безпеки інформації.

Згідно ДСТУ 3396.0/1-96 «ТЗІ. Основні положення (п. 3.2) можливі такі варіанти організації захисту інформації:

- досягнення необхідного рівня захисту за мінімальних затрат і допустимого рівня обмежень видів інформаційної діяльності;
- досягнення необхідного рівня захисту за допустимих затрат і заданого рівня обмежень видів інформаційної діяльності;
- досягнення максимального рівня захисту за необхідних затрат і мінімального рівня обмежень видів інформаційної діяльності.

Відомі методичні рекомендації щодо захисту інформації в АСУ орієнтовані в першу чергу на розроблювачів інформаційних систем, а не на користувачів чи системних адміністраторів або менеджерів безпеки. Водночас з практичної точки зору більш важливі рекомендації, які дають не строго оптимальне, а досить ефективне рішення щодо захисту інформації.

Сучасні методики не враховують постійної перебудови структури АСУ, що захищаються, та не містять практичних рекомендацій з формування режиму безпеки. Іншими словами, ці рекомендації не дають відповідей на два головних з практичної точки зору питання:

- Як створювати АСУ, щоб вона відповідала вимогам безпеки інформації?
- Як практично сформувати політику безпеки й підтримувати її в умовах постійної зміни конфігурації програмно-апаратних засобів й структури самої системи?

На відміну від методик технічного захисту інформації на окремих об'єктах інформаційної діяльності, виникає потреба дослідження та впровадження сучасних підходів та методичного апарату для створення систем безпеки комп'ютерно-інтегрованих технологій, які б враховували питання захисту складних процесів обробки інформації в АСУ. Тому виникає потреба дослідження методології безпеки комп'ютерно-інтегрованих технологій (КІТ) в АСУ відповідно сучасним потребам.

У якості основних тенденцій розвитку сучасних методичних підходів до захисту інформації АСУ можна зазначити:

- розвиток методик оцінки, які дозволяють простежити прямування від єдиної шкали ранжирування вимог і критеріїв безпеки до множини незалежних часткових показників і введенню частково упорядкованих шкал;
- зростання ролі вимог адекватності реалізації засобів захисту і політики безпеки що свідчить про переважання «якості» забезпечення захисту над її «кількістю»;
- визначення функцій учасників процесу створення й експлуатації захищених систем, застосування відповідних механізмів і технологій оптимального розподілу відповідальності між всіма учасниками цього процесу.

На даному етапі в АСУ багато уваги приділяється створенню комплексних систем захисту інформації. Але процес проектування та впровадження зазначених систем захисту базується на застарілих методичних підходах технічного захисту інформації, коли особлива увага приділяється збереженню конфіденційності інформації з обмеженим доступом на окремих об'єктах інформаційної діяльності.

Ускладнення технологій обробки інформації призвело до появи нових видів загроз для процесів функціонування комп'ютерних систем. Збитки та руйнації, що є наслідком реалізації загроз інформаційним технологіям, набагато більші ніж наслідки загроз витоку інформації технічними каналами.

Створення КІТ з системою безпеки (СБ) в АСУ має свої різні властивості, і перше за все, це багаторівневий взаємопов'язаний комплекс: цілей, функціональних задач, матеріальних та інформаційних потоків які потребують захисту в АСУ, алгоритмів функціонування та управління системою безпеки інформації в АСУ.

Процеси створення та впровадження СБ КІТ в АСУ характеризуються великим ступенем невизначеності, випадковості, нестабільності,

а їх відображення здійснюється системою кількісних і якісних показників, які зазвичай подаються в вербальній нечітко заданій формі.

Системи безпеки КІТ в АСУ являють собою складні організаційно-технічні системи, що мають велику вимірність і багаторівневість. У роботах по створенню таких систем безпеки, як правило, беруть участь десятки організацій та підприємств, що накладає специфічні вимоги стосовно узгодження їхніх дій.

При переході від методів проектування засобів технічного захисту інформації до складних систем безпеки виникає необхідність створення єдиної комплексної методології проектування та впровадження СБ КІТ в АСУ, яка об'єднує в собі методи розробки підсистем, елементів та програмних механізмів захисту інформації.

У цьому зв'язку в розробці СБ КІТ в АСУ, на відміну від розробки засобів технічного захисту інформації, більшу частину складають задачі системного проектування та аналізу. Це задачі декомпозиції, системного проектування різних властивостей систем безпеки, побудови математичних та системних моделей різного класу, комплексування проектних рішень, розробки технічних вимог до елементів систем, аналізу коректності проектних рішень та інше.

Оскільки СБ КІТ в АСУ має велику вимірність і багаторівневість, то провести об'єктивний та достовірний аналіз проєктних рішень на етапах системного проєктування без сучасних комп'ютерних технологій неможливо. Тому методологія та методи розробки системних етапів СБ КІТ в АСУ повинні створюватись з урахуванням їхньої подальшої реалізації комп'ютерними засобами, що, в свою чергу, потребує їхньої формалізації та розробки нової інформаційної технології проєктування.

Отже, для захисту комп'ютерно-інтегрованих технологій потрібне сумісне використання різних за функціями та складом компонентів безпеки інформації, таких як заходи, методи, засоби, механізми, процедури захисту та ін. Ці компоненти потребують об'єднання в систему безпеки комп'ютерно-інтегрованих технологій та встановлення жорстких логічних та функціональних зв'язків між собою. Захист інформації в автоматизованих системах управління технологічними процесами потребує взаємного, узгодженого та синхронізованого проєктування, впровадження та експлуатації АСУ невід'ємно від комплексної системи захисту інформації як єдиного цілого.

Список використаної літератури:

1. Розробка комплексних систем захисту інформації в сучасних інформаційно-телекомунікаційних системах. Перспективні напрями захисту інформації : матеріали першої всеукр. наук.-пр. конференції, м. Одеса 7–9 вересня 2015 р.: ОНАЗ, 2015. С. 69–73.
2. Манжай О. В., Манжай І. А. Правові засади захисту інформації: підручник. Харків : Панов, 2020. 162 с. : ISBN 978-617-7634-85-9.
3. Марченко А. В. Проєктування інформаційних систем. Київ : НТУ, 2015. 40 с. URL: http://kist.ntu.edu.ua/textPhD/PIS_Marchenko.pdf

4. Гончар С. Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом. Захист інформації. 2014. Т. 16, № 1. С. 40–46.

Ключові слова: інформація, захист інформації, автоматизована система управління, комплексна система захисту інформації, система безпеки, комп'ютерно-інтегровані технології.

Ключевые слова: информация, защита информации, автоматизированная система управления, комплексная система защиты информации, система безопасности, компьютерно-интегрированные технологии.

Key words: information, information protection, automated control system, complex information protection system, information security system, computer-integrated technologies.

БАЛАНДІНА НАТАЛІЯ МИКОЛАЇВНА

Національний університет «Одеська юридична академія», старший викладач кафедри кібербезпеки

СЛАТВІНСЬКА ВАЛЕРІЯ МИКОЛАЇВНА

Національний університет «Одеська юридична академія», аспірантка кафедри господарського права і процесу

ІНФОРМАЦІЙНА КУЛЬТУРА ІНФОРМАТИЗОВАНОГО СУСПІЛЬСТВА

Сучасне суспільство все більше набуває рис інформаційного суспільства. Становленню суспільства інформаційного типу сприяла низка технологічних проривів: винахід телеграфу, телефону, радіо, телебачення, поширення мобільного зв'язку. Сучасні інформаційні технології не тільки впливають на свідомість і поведінку людини, а й визначають в цілому життєвий стиль розвитку особистості і суспільства, характер відносин і взаємодій, а також тенденції в області розвитку економіки, політики, культури, освіти і т. п.

Винахід глобальної мережі Інтернет і мобільного зв'язку зумовили стрімкий розвиток і трансформацію інформаційно-комунікативного простору і в цілому інформатизацію суспільства. Мобільні телефони стали не тільки засобами встановлення контакту, але і зберігачем величезної кількості інформації, а також засобом інтернет-комунікації.

Сучасний інтернет впливає на динаміку соціальних змін і свідомість молоді, соціалізація якої в інформаційному суспільстві здійснюється під потужним впливом засобів масової інформації в цілому і мережі Інтернет зокрема, та формує стильові зразки, ціннісні установки, і пріоритетні моделі поведінки [1].

Інтернет має безліч позитивних і привабливих властивостей не тільки для молодого, але і для старшого покоління, серед яких