КОНЦЕПЦІЯ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ ОБРОБЛЕНННЯ ІНФОРМАЦІЇ

Говоров А.С.,
Стогул К.М.
Науковий керівник: Дмитрієв І.А., д.е.н., професор
Харківський національний автомобільно-дорожній університет

Безпека автоматизованих систем обробки інформації (АСОІ) - це її здатність протидіяти негативним впливам, що порушують її нормальне функціонування [1]. Іншими словами, під безпекою системи розуміється її захищеність від випадкового або навмисного втручання в нормальний процес її функціонування, а також спроба розкрадання, модифікації або руйнування її компонентів. Природа впливів може бути різною: це і спроба проникнення зловмисника, і помилки персоналу, природні стихійні лиха, техногенні катастрофи та аварії (пожежі, землетруси, вимкнення електроживлення), вихід з ладу складових частин системи обробки інформації.

Вимоги щодо забезпечення безпеки обчислювальних мереж, включно із захистом інформації, що зберігається та обробляється в них, спрямовані на розв'язання потрійної задачі, яка полягає в досягненні певного поєднання трьох властивостей: конфіденційності оброблюваної інформації, цілісності та доступності компонентів і ресурсів системи.

Конфіденційність інформації - це властивість інформації бути відомою тільки тим, кому вона призначена, допущеним суб'єктам системи, які пройшли перевірку. Для інших суб'єктів системи ця інформація ніби не існує.

Цілісність компонента (ресурсу) системи - це його властивість бути коректним під час функціонування системи, тобто задовольняти деяким правилам узгодженості для інформації або вимогам безпеки для програмного забезпечення.

Доступність компонента (ресурсу) - це його властивість бути готовим для використання санкціонованими суб'єктами системи в будь-який час.

Загальна модель системи забезпечення безпеки АСОІ містить у собі такі компоненти:

– об'єкти захисту, тобто компоненти АСОІ та пов'язаних з нею систем, що потребують захисту;

– загрози, потенційно можливі впливи на АСОІ, здатні порушити нормальний процес її функціонування;

– засоби захисту.

Компоненти АСОІ, які можуть бути підтверджені загрозам і робота яких може бути порушена, називаються також уразливими місцями. Один із варіантів класифікації системи на компоненти, які можуть бути піддані загрозам, включає: апаратні засоби обчислювальної техніки; програмні засоби; інформаційне забезпечення; системи зв'язку.

Уразливим місцем АСОІ можна вважати персонал, який може бути підданий впливу з боку злочинних угрупувань для отримання доступу до цінної

інформації.

Залежно від завдань, що стоять перед АСОІ, і вимог до системи безпеки можуть бути використані більш детальні поділ системи на компоненти або взагалі інші варіанти класифікації.

Безліч усіх загроз безпеці може бути розділено на три групи: природні; техногенні; з боку людини.

Найпоширеніші природні загрози - це: холодна погода, землетрус, повінь, спекотна погода, снігопади, польові бурі, проливні дощі, урагани.

До типових техногенних загроз належать: пожежі, вимкнення електроживлення, витоки газів і нафтопродуктів, вихід з ладу апаратних засобів АСОІ, радіоактивні опади, затоплення.

Загрози, пов'язані з людьми, можна розбити на дві підгрупи: загрози, зумовлені помилками персоналу; загрози, пов'язані з діями зловмисників.

Багато засобів, спрямованих на захист від загроз, пов'язаних із людським фактором, можна застосувати і для захисту від природних і техногенних загроз, але перші істотно різноманітніші, їх важко виявити і вони потребують істотно складніших засобів захисту. Це пов'язано з маскуванням порушниками своїх дій, складності їхніх дій, які можуть являти собою досить довгу і неочевидну, не пов'язану прямо з передбачуваною метою, послідовність операцій.

Під час побудови захисних механізмів АСЗІ досліджується, розробляється і впроваджується:

– спеціальні програмно-технічні компоненти системи, призначення яких забезпечення її безпеки;

– дії персоналу, який безпосередньо відповідає за забезпечення безпеки системи;

– методи проєктування, розроблення та експлуатації, орієнтовані на забезпечення безпеки.

Для забезпечення безпеки АСЗІ потрібне застосування цілісного комплексу засобів захисту, що включає дві групи: механізми і перешкоди. Рівень захищеності в системі визначається рівнем слабкої ланки в системі захисту.

Література:

1. Системи забезпечення інформаційної безпеки. Огляд. URL: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review

2. Закон України «Про захист інформації в інформаційно-комунікаційних системах» № 1089-IX від 16.12.2020. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text