

## **ОЦІНЮВАННЯ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СОЦІОТЕХНІЧНИХ СИСТЕМАХ**

**А.В. Дудатьєв, к.т.н., доцент,  
І.В. Шнайдер, студент  
Вінницький національний технічний університет**

Сучасне суспільство характеризується постійним зростанням кількості користувачів глобального інформаційного простору. Крім відомих переваг, це нажалює обумовлює інформаційну незахищеність і як наслідок виникнення певних загроз, які впливають на загальний стан як окремого об'єкта так і суспільства в цілому і можуть викликати конфліктний стан. Сучасні конфліктні ситуації характеризуються тим, що у конфліктах беруть участь складні технічні системи. Загальна теорія конфліктів, зокрема, у соціальних, соціотехнічних системах дозволяє сформулювати загальні положення щодо причин їх виникнення, протікання та методів їх вирішення. Формалізація життєвого циклу конфлікту дозволяє вирішити актуальні задачі, а саме: причини виникнення конфлікту, мету сторін, задіяних у конфлікті, компромісні дії, які можуть сприяти вирішенню конфліктної ситуації. Останнім часом актуальними є проведення так званих інформаційних атак або війн. Мета таких заходів у більшості випадків формулюється, як спроба реалізації лідерства на відповідному сегменті ринку, тобто викликана конкуренцією у боротьбі за лідерство або проведенні психологічної атаки, що характерно для сучасного тероризму. У цьому випадку

забезпечення комплексної безпеки зводиться до забезпечення інформаційної безпеки, практична реалізація якої полягає у розв'язку двох задач: безпосереднього захисту своїх інформаційних ресурсів від ймовірного несанкціонованого доступу та отримання певної інформації щодо дій своїх конкурентів з метою упередження можливих несанкціонованих дій і як наслідок зменшення негативних наслідків.

Таким чином, можна констатувати, що проблема аналізу причин виникнення конфліктних ситуацій у соціотехнічних системах та розробка методів щодо їх вирішення є актуальною, оскільки її рішення дозволить забезпечити комплексний інформаційний захист та оптимізувати процеси підготовки та прийняття управлінських рішень та мінімізувати ймовірні ризики.

Розвиток загальної теорії безпеки полягає у створенні узагальнених взаємопов'язаних положень та залежностей між складовими комплексної безпеки, такими як техногенна, економічна, екологічна тощо. Інтегральною характеристикою захищеності об'єкту є політика інформаційної безпеки (ПІБ), яка повинна підтримувати необхідний рівень захищеності у часі, тобто враховувати динамічний характер як небезпек, так і механізмів захисту.

Разом із врахуванням небезпечних, як внутрішніх так і зовнішніх чинників, вхідними параметрами для розробки ефективної ПІБ є певні вказівки та замовлення служби безпеки та її підрозділу інформаційно-аналітичної служби (ІАС). Це повністю об'єктивний процес, оскільки служба безпеки підприємства в більшості випадків є замовником ПІБ. Рішення задачі забезпечення необхідного рівня інформаційної безпеки, формалізується практично у вигляді двох задач. Рішення першої задачі, тобто оцінювання та забезпечення необхідного рівня захищеності забезпечується на етапі проектування системи захисту

інформації (СЗІ). Результатом розв'язку першої задачі є розроблена політика інформаційної безпеки та синтезована, оптимальна за певними показниками система захисту інформації.

Друга задача вирішується на етапі експлуатації СЗІ. Для організації комплексного захисту і ефективної протидії потенційним порушникам або ймовірним конкурентам, прийняття управлінських рішень щодо забезпечення ефективного функціонування об'єкту захисту повинні ґрунтуватися на результатах повного аналізу і оцінювання, існуючих і потенційних загроз. Рішення цієї задачі ускладнюється у зв'язку із суттєвою невизначеністю, яка пов'язана із динамічною природою всіх елементів системи. У зв'язку з цим ІАС повинна забезпечити впорядковане накопичення, науково обґрунтоване узагальнення і аналіз інформації відносно різних напрямів, що впливають на захист конфіденційної інформації, і на цій основі виконання прогнозу подальшого розвитку подій, їх можливий вплив на стійкість і життєспроможність об'єкту захисту. Розв'язок другої задачі виконується у площині організаційного захисту і передбачає цілу низку заходів, таких як організація служби безпеки, інформаційно - аналітичної служби тощо.

Автори запропонували метод для оцінювання та забезпечення необхідного або достатнього рівня забезпечення захисту інформаційних ресурсів з урахуванням можливих конфліктних ситуацій, що можуть виникнути у сучасних соціотехнічних системах.