УДК 004.056.53

Інна ЯРОВА, Аліса ВЛАСОВА, Наталія КУШНІРЕНКО

Національний університет «Одеська політехніка»

АНАЛІЗ НОРМАТИВНОЇ БАЗИ ДЛЯ СТВОРЕННЯ МОДЕЛІ ПОРУШНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вступ. Забезпечення захисту інформації в кіберпросторі ґрунтується в першу чергу на державній нормативно-правовій базі. Правова частина цієї бази складається із законів України, постанов Кабінету Міністрів України та деяких документів нижчого рівню. Нормативна частина (або нормативна база) являє собою сукупність ДСТУ – державних стандартів, та НД ТЗІ – нормативних документів системи технічного захисту інформації, створених ДССЗЗІ України. Одним з етапів процесу створення комплексних систем захисту інформації є розробка моделі порушника інформаційної безпеки. Цей етап є важливим з точки зору подальшого управління ризиками, адже для ефективного вибору тактик зниження ризиків та подолання наслідків реалізованих загроз необхідно чітко розуміти походження джерела загрози та вектор створюваної ним небезпеки. Визначальними вимогами до моделі порушника є адекватність, тобто відповідність моделі реальному об'єкту, та ступінь формалізації.

Мета: Дослідження нормативної бази технічного захисту інформації та визначення системи нормативних вимог для побудови адекватної формалізованої моделі порушника інформаційної безпеки.

Аналіз нормативних вимог для створення моделі порушника

Згідно із загальноприйнятою термінологією, порушник – користувач, який здійснює несанкціонований доступ до інформації [1]. Використовувана в процесі управління ризиками модель порушника – це абстрактний формалізований або неформалізований опис порушника [1]. Ступінь формалізації в даному документі не обговорюється. Таке визначення, з одного боку, позбавляє розробників КСЗІ необхідності жорсткої регламентації своїх дій. З іншого боку, формалізація процесів дозволяє узагальнювати певний досвід, підвищувати деталізацію, адекватність і точність моделі порушника, що розробляється. Аналіз державних стандартів в сфері кібербезпеки показав, що термін «порушник інформаційної безпеки» в них відсутній, принципи побудови моделі порушника в процесах управління ризиками не є стандартизованими. Єдиним державним стандартом, що містить згадку про джерела загроз, які визначаються на етапі аналізу загроз, є ДСТУ 3396.0-96. Це можна вважати непрямим вказанням на порушника інформаційної безпеки. Джерелами загроз за стандартом є «діяльність розвідок іноземних держав, а також навмисні або ненавмисні дії юридичних і фізичних осіб» [2]. Але в документі немає уточнень щодо реєстрації юридичних осіб або громадянства фізичних осіб, або будь-яких інших ознак. Отже, методологічні засади побудови моделі порушника спираються на документи більш низького рівня – відомчі НД ТЗІ. Згідно із [3], порушник – суб'єкт, який вчиняє навмисні

або випадкові дії, що створюють загрозу для інформації, або випадкова подія, внаслідок настання якої можуть реалізуватися загрози для автоматизованої системи. В процесі моделювання загроз рекомендується використовувати найнесприятливішу комбінацію ознак порушника: вважати, що порушник-суб'єкт є кваліфікованим фахівцем, який має повний обсяг інформації про систему, на яку він здійснює атаку, в тому числі про заходи її захисту. Для випадку, коли в якості порушника моделюється випадкова подія, рекомендується обирати найгірший закон розподілу відносно до системи, яка потребує захисту. Слід зазначити, що введення випадкової події в якості порушника інформаційної безпеки протирічить визначенню порушника, запровадженому в [1]. Положення [4] звужує поняття моделі порушника, концентруючись тільки на характеристиках його дій: це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т. ін. Цей перелік ознак, якими можуть бути описані дії порушника, фактично не завершений і протирічить подальшим вимогам до моделі порушника, наведеним далі в цьому документі, адже вона повинна визначати: можливу мету порушника, із градацією за ступенями небезпечності для автоматизованої системи; категорії осіб, з числа яких може бути порушник; припущення про кваліфікацію порушника; припущення про характер дій порушника. Для кожного параметру моделі порушника [4] наводить характеристики у вигляді рекомендацій. Це дозволяє створити вербально-інформаційну модель порушника, яка має доволі узагальнений вигляд внаслідок малої кількості класифікаційних ознак. Використання положення [3] дозволяє створити модель порушника з більшим ступенем деталізації, оскільки бере до уваги ймовірні дії порушника, його ресурсні можливості, рівень повноважень в системі, використовувані програмні та апаратні засоби. Але даний документ має доволі вузьку сферу застосування (призначений для систем захисту інформації для АТС), розроблений доволі давно і тому певною мірою морально застарів.

Висновок. Незважаючи на актуальність впровадження ризик-орієнтованих підходів в процеси управління інформаційною безпекою, нормативна база в сфері технічного захисту інформації демонструє неузгодженість в питаннях розробки моделі порушника інформаційної безпеки та низький рівень вимог щодо формалізації результатів.

Перелік використаних джерел.

1. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Електронний ресурс]. - Режим доступу: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024

2. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. [Чинний від 01.01.1997]. Вид. офіц. Київ, 1996. 6 с.

3. НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. [Електронний ресурс]. - Режим доступу: https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-1.1-001-99.pdf

4. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. [Електронний ресурс]. - Режим доступу: https://www.tzi.com.ua/downloads/1.4-001-2000.pdf