УДК 004.056.53

І. ЯРОВА

Національний університет Одеська політехніка

АНАЛІЗ МЕТОДИК ПОБУДОВИ МОДЕЛІ ПОРУШНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ. Побудова моделі порушника інформаційної безпеки є одним з етапів створення плану захисту інформації в автоматизованої системі, який реалізується шляхом впровадження комплексної системи захисту інформації (КСЗІ). Важливою вимогою до моделі порушника є її адекватність, тобто здатність враховувати галузеву специфіку автоматизованої системи.

Мета: дослідження шляхів вдосконалення моделі порушника інформаційної безпеки на прикладі КСЗІ електронних систем охорони здоров'я.

Аналіз принципів побудови моделі порушника інформаційної безпеки.

Згідно з Типовим положенням [1], модель порушника - це абстрактний формалізований або неформалізований опис дій порушника, який відображає певні його ознаки: ймовірну мету із її градацією за ступенями небезпечності для ІТС, можливі категорії осіб, з числа яких може бути порушник, припущення про кваліфікацію та характер дій порушника. Для кожної з цих класифікаційних ознак [1] визначає видові характеристики і в описовому вигляді надає алгоритм побудови моделі порушника. Таким чином створюється вербально-інформаційна модель порушника інформаційної безпеки, яка має доволі узагальнений вигляд внаслідок малої кількості класифікаційних ознак. На наш погляд, дана методологія формує базові принципи побудови моделі порушника, але з точки зору практичного використання є недостатньо адекватною, а з точки зору використання в навчальному процесі має низьку наочність.

Модель порушника, методика побудови якої запропонована в [2], має більш високий ступінь наочності у порівнянні із попередньою. Це досягається внаслідок табличної форми опису як класифікаційних ознак порушника, так і моделі в цілому. Кожна класифікаційна ознака має окремий опис у вигляді специфікації, що враховує всі її можливі варіанти, із рейтинговою оцінкою ефективного рівня загрози для кожного варіанта. Власне модель порушника являє собою зведену таблицю профілів можливостей порушника, в якої наведені можливі категорії порушників із позначеними характеристиками класифікаційних ознак. Незважаючи на зручне наочне представлення інформації, дана модель має певні методологічно-термінологічні недоліки. При визначенні категорій порушників в специфікації відсутнє чітке розмежування на внутрішніх і зовнішніх порушників. Також недостатньо уваги приділено категоріюванню внутрішніх порушників, адже цілком логічно, що порушення інформаційної безпеки найчастіше відбуваються саме зі сторони цієї групи користувачів системи.

При побудові моделі порушника слід брати до уваги той факт, що досягнення адекватності моделі реальним порушникам можливе тільки з урахуванням галузевих особливостей інформаційно-телекомунікаційної системи.

Розглянемо це на прикладі електронної системи охорони здоров'я, призначеної для автоматизації процесів управління медичною інформацією пацієнтів. Подібні системи забезпечують збір, обробку та зберігання персональних та медичних даних пацієнтів. Можливі категорії порушників інформаційної безпеки для подібної системи наведені в Таблиці 1. Аналогічно табличним методом задаються класифікаційні ознаки порушника, із варіантами значень і рейтинговою оцінкою кожного варіанту.

Таблиця 1 - Категорії порушників інформаційної безпеки

Код	Категорія порушника	Рівень загрози
	Внутрішні порушники	
П1	Системний адміністратор	5
П2	Фахівець інформаційної безпеки	5
П3	Інженер з обслуговування апаратно-технічних засобів ІТС	4
П4	Фахівець - інженер або технік з обслуговування комунальних систем медичної установи	2
П5	Співробітник служби фізичної охорони медичної установи	4
П6	Сімейний лікар	3
П7	Профільний лікар	3
П8	Уповноважена посадова особа НСЗУ	2
П9	Адміністратор медичних даних	4
П10	Відвідувач медичної установи	5
	Зовнішні порушники	
П11	Професійний зломщик систем охорони здоров'я	5
П12	Колишній співробітник, фахівець з інформаційних технологій	5
П13	Аутсорсінговий консультант з інформаційної безпеки	5
П14	Стороння особа, що знаходиться за межами контрольованої території медичної установи	2

Висновок. Проведені дослідження дозволяють зробити висновок, що адекватна модель порушника інформативної безпеки повинна поєднувати в собі формальні методи опису із деталізацією класифікаційних ознак.

Перелік використаних джерел.

1. 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

2. Комаров М.Ю., Ониськова А.В., Гончар С.Ф. Аналіз і дослідження моделі порушника безпеки інформації для захищеного вузла Інтернет доступу. Вчені записки ТНУ ім. В.І. Вернадського. Серія: технічні науки. Т. 29 (68). Ч. 1, № 5. 2018. С. 138 - 142. [Електронний ресурс].- Режим доступу: https://tech.vernadskyjournals.in.ua/journals/2018/5_2018/part_1/26.pdf