УДК 003.26.09

Полотай О.І.
кандидат технічних наук, доцент
Львівський державний університет безпеки життєдіяльності
Масюк Н.А.
курсант
Львівський державний університет безпеки життєдіяльності

ПРОФІЛІ МОЖЛИВОСТЕЙ ПОРУШНИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СТРУКТУРНИХ ПІДРОЗДІЛІВ БЕЗПЕКОВИХ СТРУКТУР

Порушник – це особа, яка здійснила спробу виконати дії, які призвели до порушення властивостей інформації, що визначені політикою безпеки.

В табл. 1 показані категорії можливих порушників інформаційної безпеки, що притаманні у відділі інформаційних технологій головного управління ДСНС України, незалежно від обласного підпорядкування.

Таблиця 1

Категорії порушників

Позначення	Визначення категорії	Рівень загрози
	Внутрішні у відношенні до відділу інформаційних технологій ГУ ДСНС	
ПВ1	Технічний персонал, який обслуговує будівлі та приміщення (електрики, сантехніки, прибиральники тощо), в яких розташовані компоненти ІТС.	1
ПВ2	Персонал, який обслуговує технічні засоби (інженери, техніки)	2
ПВ3	Відвідувачі	1
ПВ4	Користувачі ІТС	2
ПВ5	Співробітники підрозділів (підприємств) з розробки та супроводження програмного забезпечення	3
ПВ6	Адміністратори	3
	Зовнішні у відношенні до відділу інформаційних технологій ГУ ДСНС	
ПЗ1	Будь-які особи, що знаходяться за межами контрольованої зони	1
ПЗ3	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ4	Хакери	3
ПЗ5	Співробітники закордонних спецслужб або особи, які діють за їх завданням	4

Якщо аналізувати порушників і проводити оцінку їх можливості реалізувати загрозу, то використовуються наступні фактори, які представлені у табл. 2-6.

Таблиця 2

Специфікація моделі порушника за мотивами здійснення порушень (М)

Позначення	**Мотив порушення**	**Рівень загрози**
М1	Безвідповідальність	1
М2	Самозатвердження	2

М3	Корисний інтерес	3
М4	Професійний обов’язок	4

Таблиця 3

Специфікація моделі порушника за рівнем кваліфікації та обізнаності (К)

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загрози
К1	Знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи	1
К2	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем	2
К4	Знає структуру, функції та механізми дії засобів захисту, їх недоліки	3
К5	Знає недоліки та вади механізмів захисту, які вбудовано у системне програмне забезпечення та його недокументовані можливості	3
К6	Є розробником програмних та програмно-апаратних засобів захисту або системного програмного забезпечення	4

Таблиця 4

Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту (З)

Позначення	Характеристика можливостей порушника	Рівень загрози
З1	Використовує лише агентурні методи одержання відомостей	1
З2	Використовує пасивні засоби (технічні засоби переймання без модифікації компонентів системи)	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути приховано пронесені крізь охорону	3
З4	Застосовує методи та засоби дистанційного (з використанням штатних каналів та протоколів зв’язку) впровадження програмних закладок та спеціальних резидентних програм збору, пересилання або блокування даних, дезорганізації систем обробки інформації.	3
З5	Застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передачі даних).	4

Таблиця 5

Специфікація моделі порушника за часом дії (Ч)

Позначення	Характеристика можливостей порушника	Рівень загрози
Ч1	До впровадження ІТС відділу інформаційних технологій ГУ ДСНС України	1
Ч2	Під час бездіяльності компонентів системи (у неробочий час, під час планових перерв у роботі, перерв для обслуговування та ремонту та ін.)	2
Ч3	Під час функціонування ІТС відділу інформаційних технологій ГУ ДСНС України (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС відділу інформаційних технологій ГУ ДСНС України так і під час тимчасової зупинки компонентів системи	4

Таблиця 6

Специфікація моделі порушника за місцем дії (Д)

Позначення	Характеристика місця дії порушника	Рівень загрози
Д1	Без доступу на контрольовану територію	1
Д2	З контрольованої території без доступу у будинки та споруди	1
Д3	Усередині приміщень, але без доступу до технічних засобів ІТС відділу	2

	інформаційних технологій ГУ ДСНС України	
Д4	З робочих місць користувачів ІТС відділу інформаційних технологій ГУ ДСНС України	2
Д5	З доступом у зони даних	3
Д6	З доступом у зону керування засобами забезпечення безпеки ІТС відділу інформаційних технологій ГУ ДСНС України	4

В таблиці 7, сформовані профілі можливостей порушників всіх категорій з урахуванням зазначених вище факторів. У графі "Ефективний рівень загроз" наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Таблиця 7

Профілі можливостей порушників

Позначення	Визначення категорії	Характер дій порушника					Ефективний рівень загроз
		Мотив порушення	Кваліфікація	Можливості	Час дії	Місце дії	
Внутрішні							
КР1	Відвідувачі	М2-М3	К1-К6	З1	Ч3	Д2-Д4	1
КР2	Обслуговуючий персонал	М1-М3	К1-К2	З1	Ч3	Д2-Д5	1
КР3	Технічний персонал	М1-М3	К1-К3	З2	Ч3	Д2-Д4	2
КР4	Користувачі	М1-М3	К1-К2	З1-З2	Ч2-Ч4	Д2-Д4	2
КР5	Співробітники підрозділів супроводження програмного забезпечення	М1-М3	К1-К6	З2	Ч2-Ч4	Д2-Д5	3
КР6	Адміністратори	М1,М2	К1-К6	З2-З3	Ч1-Ч4	Д2-Д6	4
Зовнішні							
КР7	Будь-які особи, що знаходяться за межами контрольованої зони	М2-М3	К1-К3	З1-З3	Ч3	Д1	1
КР8	Представники організацій, що взаємодіють з технічного забезпечення	М2-М3	К1-К4	З1	Ч3	Д1	2
КР9	Хакери	М2-М4	К1-К6	З4	Ч3	Д1	3

Література:

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 року;

2. Петров В.А. Інформаційна безпека. Захист інформації від несанкціонованого доступу в автоматизованих системах / Петров В.А., Піскарьов С.А., Шеїн А.В. – М. : Изд-во Ореан, 1998. – 534 с.