УДК 623.618

О. В. Орел

МОДЕЛЬ ДЛЯ ВИЗНАЧЕННЯ РІВНІВ КВАЛІФІКАЦІЇ ПРАВОПОРУШНИКІВ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОЦЕСІВ СЛУЖБОВО-БОЙОВОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Висвітлено загальні аспекти визначення рівнів кваліфікації правопорушників у сфері інформаційної безпеки. Акцентовано увагу на проблемних питаннях, які виникають на сучасному етапі розвитку держави.

Ключові слова: *правопорушник, інформаційна безпека.*

Постановка проблеми. Науково-технічний прогрес, що стрімко проникає у різні сфери людської діяльності, привів до того, що у другій половині ХХ ст. поняття "інформація" набуло якісно нового значення. Із звичайного позначення відомостей, що передаються людьми усно, на письмі або іншим способом (за допомогою умовних сигналів, технічних засобів тощо), інформація перетворилася на явище, що має власну, особливу цінність. Причинами такого перетворення є, головним чином, революційні винаходи в області комп'ютерної техніки. Наслідком цих винаходів стало формування нової сфери людських відносин – інформаційної, де однією із глобальних проблем є проблема забезпечення безпеки інформації.

Особливої гостроти ця проблема набуває у діяльності органів, що мають безпосереднє відношення до завдань забезпечення безперебійної роботи державних механізмів. Важливе місце серед них посідає Міністерство внутрішніх справ України (далі – МВС) у цілому та Національна гвардія України зокрема. Діяльність Національної гвардії України (далі – НГУ) як частини єдиної правоохоронної системи нерозривно пов'язана з інтересами суспільства та держави у цій сфері.

Питання забезпечення інформаційної безпеки у діяльності НГУ мають неабияке значення. Необхідність удосконалювання організації її діяльності у напрямку забезпечення протидії будь-яким посяганням на інформацію очевидна. Це пов'язано зі значним обсягом інформації, що надходить до територіальних органів НГУ і являє собою, у міру її накопичення та систематизації, визначену цінність, яка привертає увагу різних правопорушників, кримінальних елементів або структур.

Об'єктивно існуючі уразливі місця в інформаційній діяльності територіальних органів НГУ породжують істотну проблему її безпеки. Тому одним із серйозних факторів підвищення ефективності роботи Національної гвардії України у сучасних умовах є вдосконалення механізмів забезпечення інформаційної безпеки, а саме створення моделі для визначення рівнів кваліфікації правопорушників системи інформаційної безпеки та її адаптації до поточних умов службово-бойової діяльності НГУ. Внаслідок цього виникає потреба у вивченні зазначеного питання, що обумовлює *актуальність* визначеної тематики.

Метою статті є розкриття загальних аспектів визначення рівнів кваліфікації правопорушників у сфері інформаційної безпеки. Наголошення на основних принципах і підходах, які використовуються у практичній діяльності військовослужбовців, становлять *новизну вибраної тематики*.

За даними багатьох дослідних центрів кількість правопорушень у сфері використання комп'ютерних систем та телекомунікаційних мереж рік у рік постійно зростає. Завдана шкода складає мільярди доларів США. Ситуація потребує негайного створення системи протидії цьому різновиду злочинності на державному та міждержавному рівнях.

Дослідивши причини порушень, ми можемо або вплинути на ці причини (звичайно, якщо це можливо), або точніше визначити вимоги до системи захисту від такого виду порушень або злочинів. Проте в реальних умовах загрози інформації можуть виникати як унаслідок випадкових помилок персоналу, операторів, користувачів, так і внаслідок низького рівня їхньої кваліфікації. Тому модель для визначення рівнів кваліфікації правопорушників слід будувати, виходячи з конкретної ситуації, організації мережі, технології оброблення інформації; вона має відображувати практичні і теоретичні можливості, апріорні знання, час і місце дії та ін. Для досягнення своїх цілей

порушник повинен докласти зусиль, затримати визначені ресурси.

Іншими словами, порушник – це особа, що здійснює заборонені операції (дії) помилково, через незнання або свідомо з поганим наміром (і корисливою метою) або без такого, а також у вигляді протестних дій і використовує для цього різноманітні можливості, методи та засоби.

Правопорушник – це суб'єкт (порушник), що має доступ до роботи зі штатними засобами інформаційної системи (далі – ІС) і йде на порушення з корисливою метою. Його можна класифікувати за рівнем можливостей, наданих штатними засобами інформаційної системи. Класифікація є ієрархічною, тобто кожний такий рівень містить у собі функціональні можливості попереднього.

І рівень визначає найнижчий рівень можливостей ведення діалогу в ІС – запуск задач (програм) із фіксованого набору, що реалізують заздалегідь передбачені функції з оброблення інформації.

ІІ рівень визначається можливістю створення і запуску власних програм з основними функціями з оброблення інформації.

ІІІ рівень визначається можливістю керування функціонуванням ІС, тобто впливом на базове програмне забезпечення системи, на склад і конфігурацію її обладнання.

ІV рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію та ремонт апаратно-технічних засобів ІС, аж до включення до складу робочих станцій і засобів обчислюваної техніки власних апаратних засобів із новими функціями з оброблення інформації.

На своєму рівні правопорушник є спеціалістом вищої кваліфікації, знає все про ІС і, зокрема, про систему і засоби її захисту.

Така класифікація правопорушників є корисною для використання у процесі оцінювання ризиків та аналізу вразливості інформаційної системи.

Правопорушники можуть бути внутрішніми (із числа персоналу системи) або зовнішніми (сторонніми особами).

Внутрішнім правопорушником може бути особа, що належить до таких категорій персоналу: користувачі (оператори системи); персонал, що забезпечує технічні засоби (інженери, техніки); співробітники відділів розроблення і супроводження програмного забезпечення (прикладні та системні програмісти); технічний персонал, що обслуговує приміщення (прибиральники, електрики, сантехніки та інші робітники, що мають доступ до приміщень, де розміщені компоненти системи технологічного керування); військовослужбовці, службовці або працівники НГУ; керівники різних рівнів посадової ієрархії.

Сторонні особи, що можуть бути правопорушниками: студенти, представники організацій, громадяни; відвідувачі (запрошені з будь-якого приводу); представники організацій, що взаємодіють із питань забезпечення життєдіяльності підрозділів НГУ (енерго-, водо-, теплопостачання та ін.); представники конкуруючих відомств, структур та організацій (іноземних служб) або особи, що діють за їхнім завданням; особи, що випадково або навмисно порушили пропускний режим (не маючи на меті порушити безпеку); будь-які особи за межами контрольованої території.

Усіх правопорушників можна класифікувати за такими характеристиками.

1. За рівнем знань комп'ютерної системи: правопорушник знає функціональні особливості комп'ютерної системи (далі – КС), основні закономірності, формування у ній масивів даних та потоків, запитів до них; уміє користуватися штатними засобами; має високий рівень знань і значний досвід роботи з технічними засобами та системами їх обслуговування; володіє високим рівнем знань в області програмування й обчислюваної техніки, проектування й експлуатації КС; знає структуру, функції та механізм дії засобів захисту КС, їх сильні і слабкі сторони.

2. За рівнем можливостей (методів і засобів, які використовуються): правопорушник, який використовує суто агентурні методи одержання даних; використовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи); використовує тільки штатні засоби і недоліки систем захисту для їхнього подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні носії інформації, що можуть бути таємно внесені через пости охорони; використовує методи і засоби активного впливу (модифікація і підключення додаткових технічних засобів, підключення до каналів передачі даних, введення програмних закладок і використання спеціальних інструментальних та технологічних програм).

3. За часом дії: у процесі функціонування компонентів комп'ютерної системи (у неробочий час, під час планових перерв у роботі, перерв для обслуговування, ремонту тощо); як у процесі функціонування КС, так і у період неактивності компонентів системи.

4. За місцем дії: без доступу на контрольовану територію організації (підрозділу); з контрольованої території без доступу до помешкань та споруд; усередині помешкань, але без доступу до КС; з робочих місць віддалених користувачів (операторів) КС; з доступом у зону даних (баз даних, архівів та ін.); з доступом у зону користування засобами забезпечення безпеки КС.

Сьогодні правопорушники (хакери) об'єднуються в угруповання, а сучасний розвиток комунікативних технологій дозволяє їм миттєво обмінюватися інформацією про виявлені уразливості, розповсюджувати програмну продукцію, що дає змогу зламувати веб-сервери.

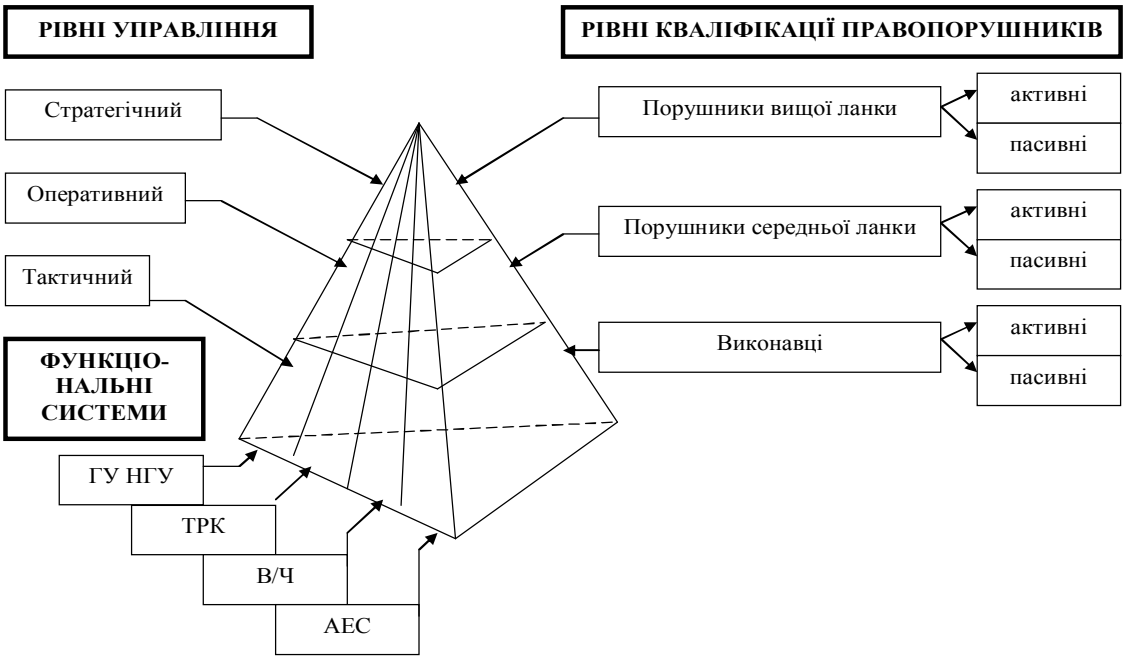
Інтернет дозволяє успішно об'єднуватися у віртуальному просторі, при цьому залишатися недосяжними у фізичному.

Найбільш небезпечними та сильними правопорушниками (хакерами) можуть стати представники військових відомств та спецслужб різних держав. Ці відомства мають потужні комп'ютери та високопродуктивні пропускні канали зв'язку. При цьому слід урахувати також той факт, що у відомствах можуть нести службу (працювати) недобросовісні військовослужбовці (співробітники або працівники), які зацікавлені у підриві репутації або завданні збитку НГУ.

Таким чином, модель для визначення рівнів кваліфікації правопорушників системи інформаційної безпеки процесів службово-бойової діяльності Національної гвардії України відображує можливі наслідки їх дій (аналіз ризиків), має характер прогнозу і розробляється на основі накопиченого досвіду, але орієнтована на майбутнє (рисунок).

У процесі розроблення моделі правопорушника слід ураховувати досвід інформативного протиборства у збройних локальних конфліктах, досвід протидії організованим злочинним угрупованням за останні 20 років, досвід захисту від хакерських атак на військові, фінансові та інші об'єкти, факти шпигунства, прогресивний розвиток мікропроцесорної, обчислювальної техніки тощо.

Модель має бути не одна, доцільно побудувати кілька відмінних моделей для визначення різних типів супротивників інформаційної безпеки процесів службово-бойової діяльності НГУ. З метою побудови такої моделі слід використовувати інформацію від служб безпеки та аналітичних груп про існуючі засоби доступу до інформації та її обробки; можливі способи перехоплення даних на стадіях передачі, оброблення та зберігання; обстановку у колективі та на об'єкті захисту тощо. Також варто оцінювати реальні оперативні технічні



Модель для визначення рівнів кваліфікації правопорушників системи інформаційної безпеки процесів службово-бойової діяльності НГУ

можливості правопорушника для впливу на систему захисту або на об'єкт, який захищається. Під технічними можливостями розуміється перелік різних технічних засобів, які може мати правопорушник у процесі вчинення дій, що спрямовані проти системи інформаційного захисту.

Типи правопорушників можуть дуже різнитися, варіюватися за складом, можливостями та цілями, які вони ставлять. Від поодинокого правопорушника, що діє віддалено і приховано, до добре озброєної та оснащеної силової групи, яка діє миттєво та напролом. Варто враховувати також можливості змови між правопорушниками, що належать до різних типів, а також підкупу та реалізації інших методів впливу.

Висновок

Отже, можна з упевненістю стверджувати, що модель для визначення рівнів кваліфікації правопорушників повинна відображувати їх практичні та теоретичні можливості, апріорні знання, фінансовий, технічний, ресурсний потенціали. У кожному випадку для системи радіозв'язку, що використовується у контурі управління, та конкретної обстановки потрібно визначати модель правопорушника, який може діяти під час виконання Національною гвардією України службово-бойових завдань. У процесі розроблення моделі необхідно визначити: категорію осіб, до яких належить правопорушник, мотиви його дій, кваліфікацію та технічне оснащення, можливу мету.

Напрямом подальших досліджень може бути побудова моделі для визначення загроз системі інформаційної безпеки НГУ, підґрунтям якої є модель для визначення рівнів кваліфікації правопорушників, які можуть діяти під час виконання Національною гвардією України завдань службово-бойової діяльності за призначенням.

Список використаних джерел

1. Философский словарь [Текст] / под ред. И. Т. Фролова. – 6-е изд., перераб. и доп. – М. : Политиздат, 1991. – 559 с.

2. Дагель, П. С. Субъективная сторона преступления и её установление [Текст] / П. С. Дагель, Д. П. Котов. – Воронеж : Изд-во Воронеж. ун-та, 1974. – 243 с.

3. Про захист інформації в автоматизованих системах [Текст] : Закон України від 5 липня 1994 р. № 25941-IV // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.

4. Положення про технічний захист інформації в Україні [Текст] : [затв. Указом Президента України від 27 вересня 1999 р. № 1229/99] // Офіційний вісник України. – 1999. – № 39. – Ст. 1934.

5. Общие положения по защите информации в компьютерных системах от несанкционированного доступа [Текст] : НД ТЗИ 1.1-002-99 // Безопасность информации. – 1999. – № 1. – С. 8–18.

6. Про інформацію [Текст] : Закон України від 2 жовтня 1992 р. № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

Стаття надійшла до редакції 11.05.2015 р.

Рецензент – доктор військових наук, професор Г. А. Дробаха, Національна академія Національної гвардії України, Харків, Україна