УДК 004.056.53

Комаров М.Ю.
Інститут проблем моделювання в енергетиці імені Г.Є. Пухова НАН України

Ониськова А.В.
Інститут проблем моделювання в енергетиці імені Г.Є. Пухова НАН України

Гончар С.Ф.
Інститут проблем моделювання в енергетиці імені Г.Є. Пухова НАН України

АНАЛІЗ І ДОСЛІДЖЕННЯ МОДЕЛІ ПОРУШНИКА БЕЗПЕКИ ІНФОРМАЦІЇ ДЛЯ ЗАХИЩЕНОГО ВУЗЛА ІНТЕРНЕТ ДОСТУПУ

У роботі здійснено аналіз і дослідження моделі порушника безпеки інформації для захищеного вузла Інтернет доступу. Подано загальну класифікацію порушників безпеки інформації, яка циркулює в захищеному вузлі Інтернет доступу. Приведено специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності, за показником можливостей використання засобів для реалізації загроз, за часом дії, за місцем дії. Показано, що розробка адекватної й максимально всеохоплюючої моделі порушника безпеки інформації є обов'язковим етапом під час побудови захищеного вузла Інтернет доступу. З'ясовано, що реалізація цього етапу дасть змогу убезпечити його ресурси, в тому числі інформаційні, від деструктивного впливу порушника будь-якого типу.

Ключові слова: *загроза, модель порушника, безпека інформації, програмне забезпечення, захищений вузол Інтернет доступу.*

Постановка проблеми. Захищений вузол Інтернет доступу (далі – ЗВІД) призначений для надання органам державної влади й органам місцевого самоврядування, державним підприємствам, установам, організаціям, іншим юридичним і фізичним особам послуг зв'язку, послуг захищеного доступу до ресурсів і сервісів мережі Інтернет.

Для захисту інформації, що обробляється та зберігається у ЗВІД, розробляється комплексна система захисту інформації (далі – КСЗІ).

КСЗІ ЗВІД призначена для:

– захисту цілісності й доступності транзитної інформації, яка передається через ЗВІД, та інформації WEB-ресурсів, які циркулюють у ЗВІД;

– захисту конфіденційності, цілісності й доступності технологічної інформації компонентів ЗВІД і технологічної інформації комплексу засобів захисту ЗВІД;

– розмежування доступу користувачів, адміністраторів і технічного обслуговуючого персоналу до інформаційних ресурсів ЗВІД;

– блокування несанкціонованих дій з транзитною інформацією, яка передається через ЗВІД, та інформацією WEB-ресурсів, які циркулюють у ЗВІД;

– захисту інформаційних ресурсів, які циркулюють у ЗВІД, від несанкціонованого доступу та модифікації;

– реєстрації спроб реалізації загроз інформації та сповіщення адміністраторів безпеки про факти несанкціонованих дій з об'єктами захисту ЗВІД.

Одним із етапів створення комплексної системи захисту інформації є розробка моделі порушника безпеки інформації.

Аналіз останніх досліджень і публікацій. Згідно з нормативними документами системи технічного захисту інформації (НД ТЗІ 1.1-002-99 [1], НД ТЗІ 1.4-001-2000 [2], НД ТЗІ 1.6-003-04 [3], НД ТЗІ 3.7-003-05 [4]), здійснюється загальна класифікація порушників безпеки інформації. Разом із тим відсутня узагальнена модель порушника безпеки інформації, яка циркулює у ЗВІД, з урахуванням практичних і потенційних можливостей, апріорних знань, часу та місця дії тощо.

Постановка завдання. Необхідно проаналізувати й дослідити модель порушника безпеки інформації, яка циркулює у ЗВІД. Під розробкою моделі порушника будемо розуміти класифікацію порушників, їх перелік, наслідки впливу.

Виклад основного матеріалу дослідження. Згідно з нормативними документами системи технічного захисту інформації [1–4], загрози безпеки інформації за локалізацією джерела загрози поділяються на внутрішні та зовнішні. До зовнішніх належать загрози, джерело яких знаходиться поза межами ЗВІД. Внутрішні загрози реалізуються в

Таблиця 1

Категорії порушників, що визначені в моделі

Позначення	Визначення категорії	Потенційний рівень загрози
П1	Системний адміністратор ЗВІД	5
П2	Адміністратор безпеки	5
П3	Користувачі	4
П4	Відвідувачі	2
П5	Технічний персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти ЗВІД	3
П6	Персонал, який обслуговує технічні засоби (інженери, техніки)	3
П7	Представники організацій, що взаємодіють з питань обслуговування ЗВІД, технічного забезпечення та підтримки її функціональності	3
П8	Сторонні особи, що знаходяться за межами контрольованої території вузлів ЗВІД	2

межах контрольованої зони, в приміщеннях, де розташовані засоби обробки та збереження інформації ЗВІД. Відповідно до цього, розрізняються два види порушників: зовнішній і внутрішній. Розглянемо кожний із зазначених видів порушників детальніше.

Зовнішній порушник – це порушник, що діє із зовнішнього щодо ЗВІД боку. У цій моделі розглядається особа, що не має доступу до приміщень, у яких розташовані засоби обчислювальної техніки, і не є авторизованим користувачем. Зовнішній порушник має можливість реалізувати загрозу інформації тільки впливаючи на інформацію з боку інших автоматизованих систем (що не входять до складу ЗВІД).

Категорії осіб, які можуть бути зовнішніми порушниками:

– сторонні особи, що знаходяться за межами контрольованої території вузлів ЗВІД;

– відвідувачі;

– представники організацій, що взаємодіють з питань обслуговування ЗВІД, технічного забезпечення та підтримки її функціональності.

Внутрішній порушник – це порушник, що діє зсередини ЗВІД. У цій моделі розглядається особа, що має доступ до приміщень, у яких розташовані засоби обчислювальної техніки ЗВІД. Внутрішній порушник має можливість реалізувати загрозу інформації й може бути як авторизованим користувачем, так і неавторизованим.

Внутрішнім порушником може бути особа з таких категорій персоналу організації:

– системний адміністратор ЗВІД;

– адміністратор безпеки;

– користувачі;

– технічний персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти ЗВІД;

– персонал, який обслуговує технічні засоби (інженери, техніки).

Потенційним порушником безпеки інформації ЗВІД є особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим наміром або без нього, використовуючи різні можливості, методи та засоби, здійснила спробу виконати операції, що призвели або можуть призвести до порушення конфіденційності, цілісності й доступності інформації.

Основним припущенням, що зроблене під час аналізу потенційного порушника для ЗВІД, є те, що адміністратор з безпеки має найвищий рівень довіри з погляду забезпечення захисту інформації ЗВІД і розглядається як особа, відповідальна за стан захищеності інформації, що обробляється в межах об’єкта, в моделі порушника не розглядається як потенційний порушник, а заходи, що можуть бути прийняті для забезпечення контролю його дій з боку керівництва, розглядаються як додаткові.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час і місце дії тощо.

Визначення категорій порушників, що прийняті в моделі, узагальнено й подано в таблиці 1. У таблицях 2–6 узагальнено й подано специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо ЗВІД, за показником можливостей використання засобів ЗВІД для реалізації загроз, за часом дії, за місцем дії. У графі «Рівень загроз» зазначених таблиць наведено рейтингову оцінку загроз порушника (можливих збитків). Рівень загрози характеризується такими категоріями:

Таблиця 2

Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Ефективний рівень загрози
М1	Безвідповідальність (недбалість)	3
М2	Корислива цілеспрямованість	5

Таблиця 3

Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ЗВІД

Позначення	Основні кваліфікаційні ознаки порушника	Ефективний рівень загрози
К1	Не володіє знаннями та інформацією про порядок функціонування ЗВІД, не має навичок щодо користування штатними засобами системи	1
К2	Має навички щодо користування ПК на рівні користувача	2
К3	Володіє базовими знаннями щодо функціонування програмного забезпечення й операційних систем і практичними навичками роботи із засобами, що реалізовані у ЗВІД	4
К4	Володіє знаннями щодо функціонування засобів і механізмів захисту, що використовуються у ЗВІД, і їх недоліки	5

Таблиця 4

Специфікація моделі порушника за показником можливостей використання засобів ЗВІД для реалізації загроз

Позначення	Характеристика можливостей порушника	Ефективний рівень загрози
З1	Має фізичний доступ до автоматизованого робочого місця ЗВІД, але не є авторизованим користувачем ЗВІД	1
З2	Має можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації	3
З3	Має можливість керування функціонуванням елементів ЗВІД, тобто конфігурує програмне забезпечення та комплекс засобів захисту ЗВІД	5
З4	Не має доступу фізичного доступу до ресурсів ЗВІД	1

Таблиця 5

Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Ефективний рівень загрози
Ч1	Під час бездіяльності компонентів системи (під час планових перерв у роботі, у неробочий час)	4
Ч2	Під час функціонування ЗВІД	5
Ч3	Під час перерв у роботі для обслуговування та ремонту	3

Таблиця 6

Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Ефективний рівень загрози
Д1	Усередині будівлі та приміщень, але без доступу до технічних засобів ЗВІД	1
Д2	З робочих місць користувачів	5
Д3	З інших об’єктів ЗВІД, у тому числі каналів зв’язку	2

1 – незначний (низький),
2 – нижчий за середній,
3 – середній,
4 – вищий за середній,
5 – значний (високий).

Модель порушника, яку побудовано з урахуванням особливостей ЗВІД (що забезпечує певне виконання технологічних процесів створення об’єкта), технологій обробки інформації, категорій персоналу й користувачів, характеризується сукупністю значень характеристик, що наведені

Таблиця 7

Профілі можливостей порушників

Позначення	Визначення категорії	Характер дій порушника					Ефективний рівень загроз
		Мотив порушення	Кваліфікація	Можливості	Час дії	Місце дії	
П1	Системний адміністратор ЗВІД	М1, М2	К4	З3	Ч1-Ч3	Д2, Д3	5
П2	Адміністратор безпеки ЗВІД	М1, М2	К4	З3	Ч1-Ч3	Д2, Д3	5
П3	Користувачі	М1, М2	К2-К4	З3	Ч1-Ч3	Д2, Д3	4
П4	Відвідувачі	М1, М2	К1-К4	З1	Ч2	Д2, Д3	3
П5	Технічний персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти ЗВІД	М1, М2	К1-К4	З1	Ч1-Ч3	Д2	2
П6	Персонал, який обслуговує технічні засоби (інженери, техніки)	М1, М2	К1-К4	З2	Ч1-Ч3	Д2	3
П7	Представники організацій, що взаємодіють з питань обслуговування ЗВІД, технічного забезпечення та підтримки її функціональності	М1, М2	К1-К4	З3	Ч1-Ч3	Д3	5
П8	Сторонні особи, що знаходяться за межами контрольованої території вузлів ЗВІД	М2	К1-К4	З4	Ч1-Ч3	Д3	1

вище. Сукупність цих характеристик визначає профіль можливостей порушника.

Профілі можливостей порушників усіх категорій подано в таблиці 7. У графі «Ефективний рівень загроз» наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Висновки. Досліджені в роботі види порушників безпеки інформації, яка циркулює у ЗВІД, засвідчують, що теоретично до цієї категорії може бути зараховано будь-якого адміністратора, користувача й технічний (обслуговуючий) персонал, який так чи опосередковано має доступ до обладнання, програмного забезпечення чи інформації, що обробляється у ЗВІД. Розробка адекватної та максимально всеохоплюючої моделі порушника під час побудови ЗВІД є обов'язковим етапом, реалізація якого дасть змогу убезпечити його ресурси, в тому числі інформаційні, від деструктивного впливу порушника будь-якого типу.

Список літератури:

1. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
2. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
3. НД ТЗІ 1.6-003-04. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.
4. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

АНАЛИЗ И ИССЛЕДОВАНИЕ МОДЕЛИ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ ЗАЩИЩЕННОГО УЗЛА ИНТЕРНЕТ ДОСТУПА

В работе осуществлены анализ и исследование модели нарушителя безопасности информации для защищенного узла Интернет доступа. Приведена общая классификация нарушителей безопасности информации, циркулирующей в защищенном узле Интернет доступа. Приведены спецификации модели нарушителя по мотивам совершения нарушений, по уровню квалификации и осведомленности, по показателю возможностей использования средств для реализации угроз, по времени действия, за местом действия. Показано, что разработка адекватной и максимально всеобъемлющей модели нарушителя

безопасности информации является обязательным этапом при построении защищенного узла Интернет доступа; что реализация данного этапа позволит обезопасить его ресурсы, в том числе информационные, от деструктивного влияния нарушителя любого типа.

Ключевые слова: *угроза, модель нарушителя, безопасность информации, программное обеспечение, защищенный узел Интернет доступа.*

ANALYSIS AND RESEARCH OF THE MODEL OF INFORMATION SECURITY VIOLATOR FOR A SECURED INTERNET ACCESS NODE

The paper analyzes and researches the model of the information security violator for a secured Internet access node. The general classification of information security violators circulating in a secured Internet access node is given. The specifications of the violator model based on violations, on the level of qualification and awareness, on the indicator of possibilities of using means for realization of threats, by time of action, by place of action are given. It is shown that the development of an adequate and the most comprehensive model of information security violator is an obligatory stage in construction of a secured Internet access node. It is shown that realization of this stage will allow to secure its resources, including information, from the destructive influence of the violator of any type.

Key words: *threat, violator model, information security, software, secured Internet access node.*