© Kireienko O. Information security violator model with general and specialized information // Ukrainian Scientific Journal of Information Security, 2019, vol. 25, issue 1, pp. 24-29.

DOI: 10.18372/2225-5036.25.13198

РЕКОМЕНДАЦІЇ ЩОДО РОЗРОБКИ МОДЕЛІ ПОРУШНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІЗ ЗАГАЛЬНОЮ ТА СПЕЦІАЛІЗОВАНОЮ ІНФОРМАЦІЄЮ

Олександр Кіреєнко

НТУУ «Київський політехнічний інститут імені Ігоря Сікорського»

КІРЄЄНКО Олександр Володимирович

Рік та місце народження: 1993 рік, м. Київ, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2016 рік.
Посада: асистент.
Наукові інтереси: Інформаційна безпека, теорія ігор.
Публікації: "*МОДЕЛЬ ПОРУШНИКА В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ*" *Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні.*
"МУЛЬТИФАКТОРНА МОДЕЛЬ ПОРУШНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ" Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні.
E-mail: kirealex12@gmail.com.
Orcid ID: 0000-0001-9184-6738.

Анотація. *У даній статті надано рекомендації щодо розробки моделі порушника з інформацією, що відрізняється за рівнем спеціалізованості. Інформацію більш високого (загального) рівня простіше переносити з однієї моделі до іншої (або з однієї версії моделі до наступної), в той час як спеціалізована інформація використовується для кількісних оцінок збитків від проведення атаки. Різним рівням деталізованості інформації про порушника відповідають різні набори засобів захисту (відношення "багато до одного" для рівня організації, "один до одного" для рівня філіалу, "один до багатьох" для рівня поточної версії системи). Розроблена відповідно до наданих рекомендацій модель порушника дозволяє враховувати рівень контролю порушника за проведенням атаки та пріоритет вибору цілей для атаки.*

Ключові слова: *захист інформації, модель порушника, сценарії атаки, загрози, імовірність мотивації порушника, імовірність проведення успішної атаки, неоднорідна інформація, подібність атак.*

Вступ

Згідно з НД ТЗІ 1.1-003-99

Модель порушника (userviolatormodel) — абстрактний формалізований або неформалізований опис порушника.

Сторона захисту розробляє модель порушника з урахуванням специфіки функціонування системи, яку планують захищати. Модель порушника використовується для оцінювання рівня загроз, виявлення слабких місць в системі, прогнозування атаки/послідовності атак, а також сценаріїв відновлення системи після успішно проведеної атаки. Інформація, що міститься в моделі, може бути неоднорідною (відрізняється формат представлення даних, точність, достовірність).

В цій статті надано рекомендації щодо розробки моделі порушника з неоднорідною інформацією. Основною причиною неоднорідності є різний рівень спеціалізованості інформації. Модель порушника може містити загальну інформацію, що є однаковою для декількох організацій та окремих користувачів ПК, інформацію, що є специфічною для конкретної галузі (банківська сфера, державні установи, медицина), інформацію, що є специфічною для конкретної організації в межах даної галузі (загрози пов'язані із промисловим шпигунством, інсайдерські загрози), інформацію, що характерна для конкретної установи (специфіка географічного розміщення, попередні атаки та події, що стали дестабілізуючими факторами), інформацію, що відноситься лише до поточної версії системи в межах окремої установи (особливості налаштування обладнання, обізнаність персоналу, установлені патчі).

Якщо модель порушника містить інформацію з різними рівнями спеціалізованості, це ускладнює перенесення інформації з однієї моделі порушника до іншої у випадках, коли кількість рівнів в даних моделях не співпадає, або відрізняються критерії, за якими інформація відноситься до того чи іншого рівня. Розбиття інформації на рівні потрібно здійснювати таким чином, щоб інформацію більш загального рівня можна було переносити між моделями без жодних змін (дві організації в межах однієї галузі мають однаковий набір даних загального рівня, філіали однієї організації матимуть однакову інформацію рівня організації і вище). Малі організації (представлені лише 1 філіалом) можуть використовувати інформацію рівня філіалу із іншої моделі в якості інформації рівня організації у власній моделі.

Аналіз існуючих досліджень

В роботі [1] проведено логістичний регресивний аналіз для встановлення зв'язку між рівнем загрози та різними факторами (кількість вузлів, що мають E-mail адресу, кількість галузей, з якими пов'язана система даного підприємства, механізми захисту, політика безпеки, персонал). В роботі [2] описано рефлексивні моделі ризиків та дано оцінки інтегральних ризиків для різних типів порушників. Робота [3] присвячена захисту інформації в розподілених мережах. Дана робота містить рекомендації щодо використання VPN, а також визначає функціональні послуги безпеки для таких систем. В роботі [4] надано рекомендації щодо розробки політики інформаційної безпеки (ПІБ). Модель порушника визначено як один із 3 напрямків побудови ПІБ.

Метою даної роботи є розробка моделі порушника, що орієнтована на систему з ієрархічною структурою (організація, філіали, лінії зв'язку між філіалами).

Актуальність даної роботи полягає в економії ресурсів та часу, необхідних при перенесенні інформації із однієї моделі порушника до іншої (або із однієї версії моделі до наступної), за умови, що обидві моделі (або обидві версії однієї моделі) побудовані відповідно до однакових рекомендацій.

Новизна даної роботи полягає в представленому в цій статті поділу всієї інформації в моделі на 5 рівнів, та обгрунтуванні саме такого поділу.

Зв'язок між рівнями деталізації інформації

Сторона захисту не повинна ігнорувати інформацію про порушника, що є **загальною**. Порушник може здійснити атаку на систему незалежно від задач, які дана система вирішує, без будь-якої прив'язки до часу (атака може відбутися під час штатного функціонування системи або під час оновлення). Поширення перших комп'ютерних вірусів, а також розсилання спаму можна вважати загрозами, що відносяться саме до загального рівня. Сюди ж можна віднести інформацію про порушників, що націлені на персональні комп'ютери користувачів. Низький рівень комп'ютерної грамотності та неповнота організаційних заходів захисту можуть призвести до компрометації системи шкідливим ПЗ, що не призначалося для цього. Працівник організації може принести з дому заражені файли на змінному носії і запустити їх на робочому комп'ютері. Також, не можна виключати імовірність завантаження шкідливого ПЗ із мережі при нецільовому використанні робочого комп'ютеру.

Інформація про порушника, що є **специфічною для галузі** відрізняється від загальної тим, що ціль порушника вже частково визначена. У випадку із **загальною інформацією**, сторона захисту "визнає", що інформаційна система нашої організації може стати ціллю атаки просто через використання конкретного типу носіїв інформації (віруси, що передавалися на дискетах), або конкретного обладнання (IBM-сумісні комп'ютери). **Галузева інформація** описує порушників, що в деякій мірі зацікавлені в діяльності нашої організації. В роботі [1] виділено 27 галузей (із них 14 - промислові). Дана класифікація не єдина. Приведені в роботі [1] галузі можна розбити для більшої деталізації (наприклад, розбити галузь із усіма комунальними послугами на галузі газопостачання, водопостачання та енергопостачання). Для нас важливим є факт, що кількість галузей обмежена. Для кожної галузі існує свій характерний набір порушників. Порушник, що модифікує інформацію про свою заборгованість по комунальним послугам, відрізняється від порушника, що викрадає персональні дані про стан здоров'я з метою подальшого шантажу. Також відрізнятиметься і відношення порушників різних типів. Рівень комп'ютерного піратства в галузі цифрової дистрибуції відео- та аудіоматеріалів може не співпадати з рівнем піратства електронних книг.

Потрібно пам'ятати, що інформація про порушників **галузевого рівня** вказує на можливість проведення деякої атаки на **нашу** систему. Модель порушника має враховувати факт існування інших організацій, що задіяні в одній галузі з нашою.

На рівні галузевої інформації модель може містити:

– інформацію, зібрану стороною захисту;

– інформацію, що була отримана від організацій-партнерів;

– інформацію, що була отримана від конкурентів (інформація про порушників, що створюють загрозу для всієї галузі).

Інформація про порушників-конкурентів буде розподілена між двома рівнями (рівень галузі та рівень організації). В роботі [2] імовірність виникнення збитків є добутком імовірності мотивації порушника P_t та імовірності проведення успішної атаки P_v. Інформацію щодо цілеспрямованих атак порушників-конкурентів саме на нашу систему потрібно віднести до **рівня організації** (в цьому випадку імовірність мотивації порушника $P_t = 1$). Якщо порушник може обрати іншу ціль для атаки, то $P_t < 1$.

При роботі із інформацією про порушника на галузевому рівні потрібно враховувати **подібність** атак.

Ознаками подібності можуть бути:

– тривалість атаки (якщо атака проводиться саме на систему, а не на інформацію, що в ній зберігається/обробляється, то при однаковій тривалості атаки більші системи зазнають більших збитків, так як збитки будуть пропорційні кількості вузлів що простоюють в результаті атаки/відновлення після атаки);

– витрачені на проведення атаки ресурси (при однаковій кількості затрачених на атаку ресурсів найбільші збитки *від атаки* будуть в незахищених систем);

– кількість цілей (значення може бути абсолютним або відносним, коли атака вражає деякий відсоток вузлів в системі).

На рівні галузі порушник **спочатку** обирає інформаційний актив, що його цікавить (напр. персональні дані клієнтів фін. установ або обчислювальні ресурси комп'ютерів), а вже після цього систему, в якій цей актив присутній.

Організації, що діють в межах однієї галузі можуть суттєво відрізнятися за рівнем інформаційної безпеки (бюджет, виділений на інформаційну

безпеку, рівень ризику, що можна вважати прийнятним, рівень комп'ютерної грамотності працівників, частота резервного копіювання, відсоток ліцензійного ПЗ та ін.). Відповідно можуть відрізнятися і способи проведення атаки, хоча ціль атаки буде однаковою. Інформацію про порушника галузевого рівня бажано використовувати для прогнозування типів атак (атаки на конфіденційність, цілісність, доступність).

Інформація про порушника рівня організації дозволяє стороні захисту оцінювати загрози, що спрямовані безпосередньо на нашу інформаційну систему. В даному випадку, стороні захисту відома ціль атаки (інформаційний актив/вузол в системі/канал передачі інформації/система як ціле) та, в деякій мірі, **мотив** проведення атаки. Якщо у випадку із інформацією галузевого рівня ми допускаємо, що порушник просто вибрав нашу систему випадковим чином із деякої множини цілей, то у випадку з інформацією рівня організації ми можемо додати до моделі запис про мотив порушника. Саме на цьому рівні в моделі міститься інформація про порушників, що діють від імені конкурентів, порушників, що були колишніми працівниками, і діють з метою помсти, порушників, що проводять атаку в якості підготовчого етапу іншої атаки (напр. атака, що установлює backdoor в нашій системі, атака, що перетворює нашу систему на botnet).

На даному етапі розробки моделі порушника потрібно розрізняти три підмножини загроз:

1) загрози в межах всієї організації;

2) загрози окремому філіалу, що у випадку реалізації поширяться за межі філіалу;

3) загрози лініям зв'язку між філіалами.

Загрози в межах організації – це загрози для деякого спільно використовуваного ресурсу (за винятком ліній зв'язку). Якщо організація має власний центр сертифікації, його компрометацію можна вважати загрозою для всієї організації. Відкликання сертифікатів не призведе до втрати зв'язку між філіалами організації, але ускладнить аутентифікацію сторін.

При ієрархічній структурі організації, компрометація головного офісу дозволить порушнику поширити свій вплив на підзвітні філіали. Скомпрометований філіал протягом деякого часу буде відсилати недостовірні звіти до головного офісу. Також, можливим є сценарій поширення шкідливого ПЗ із використанням ЦП (та будь-яких інших засобів аутентифікації) скомпрометованого філіалу.

Компрометація одного із філіалів може зашкодити організації, якщо даний філіал використовувався для розподіленого зберігання інформації. Одним із способів гарантування узгодженості даних при розподіленому зберіганні є правило "простої більшості". Якщо із N вузлів на N-1 зберігається один набір даних, а на останньому – відмінний від решти набір даних, то розумним є припущення про компрометацію саме цього одного вузла, а не N-1 вузлів. При малих N компрометація одного вузла стає більш загрозливою. Зниження доступності інформації (додаткові витрати часу на звернення до не скомпрометованого вузла) може спричинити затримки в бізнес-процесах організації та втрати репутації у своїх клієнтів. Повна втрата даних, що зберігалися лише на серверах скомпрометованого філіалу, теж матиме негативні наслідки.

Атака на лінії зв'язку за означенням не може бути локалізована в межах одного філіалу. Єдиним винятком з цього правила будуть філіали, що використовують односторонні лінії зв'язку (лише одна лінія симплексного зв'язку; дві різнонаправлені лінії симплексного зв'язку можуть замінити дуплексний зв'язок).

Для зв'язку між філіалами організація може використовувати VPN [3]. VPN забезпечує надлишковість, за рахунок наявності паралельних каналів передачі інформації. Використання мережі загального користування також дозволяє перекласти частину відповідальності на третю сторону (провайдера). Якщо лінії зв'язку є частиною системи, яку захищають (тобто входять до списку активів організації[4]), і відповідальність за їх відновлення лежить на нас, то для зниження збитків від атак на лінії зв'язку сторона захисту може:

а) підвищити швидкість відновлення пошкоджених/скомпрометованих ліній зв'язку;

б) підвищити стійкість ліній зв'язку до компрометації;

в) підвищити рівень автономності філіалів.

Інформація про порушника рівня філіалу є більш деталізованою і містить чіткі обмеження, з якими працюватиме сторона захисту:

- персонал;
- апаратне забезпечення;
- програмне забезпечення;
- режим роботи.

Організація може відправляти своїх працівників у відрядження, а також тимчасово залучати до роботи додатковий персонал. В межах окремого філіалу перерозподіл обов'язків персоналу суттєво обмежений. В межах філіалу може не бути спеціалістів, що відповідають за відновлення системи після успішної атаки та спеціалістів, що займаються розслідуванням інцидентів кібербезпеки. Швидкість відновлення системи після атаки залежить, в тому числі, і від кількості працівників, яких можна переназначити на відповідні роботи, а також від їх можливостей працювати понаднормово.

Кількісна та якісна нестача обладнання в межах філіалу є дестабілізуючим фактором. Якщо для відновлення роботи потрібно залучати ресурси інших філіалів, то це вважається загрозою рівня організації.

До обмежень програмного забезпечення можна віднести відсоток ліцензійного ПЗ, частку застарілого ПЗ, що використовується для забезпечення сумісності, а також частку ПЗ, що працює на віртуальних машинах. У випадку із неліцензійним ПЗ сторона захисту не зможе розраховувати на підтримку від виробника. Використання неліцензійного ПЗ також не дозволить **перекласти** ризик на третю сторону.

Режим роботи філіалу задає обмеження на ремонт та планове обслуговування обладнання, установку оновлень, резервне копіювання даних, частоту відправки звітів/лог файлів, доступність служби підтримки та інші фактори.

Інформація рівня філіалу дозволяє кількісно оцінювати збитки. Для інформації **загального рівня** рівень збитку можна оцінити кількісно, якщо він пропорційний кількості уражених вузлів в нашій системі (напр. у випадку із ransomware). Для **рівня галузі** кількісні оцінки будуть малоінформативними. Сторона захисту може дати кількісну оцінку збитку, допустивши, що порушник вибере для атаки саме нашу організацію. Проблема із кількісною оцінкою галузевого рівня полягає в тому, що проведення деякої атаки на систему наших конкурентів може мати прямий чи опосередкований **позитивний** вплив для нас. Без інформації про стан захищеності системи у наших конкурентів оцінити даний опосередкований позитивний вплив неможливо.

Для оцінювання збитків на рівні організації стороні захисту одного філіалу потрібно мати доступ до інформації, що належить іншим філіалам. В найкращому випадку (інформація інших філіалів доступна) це призведе до суттєвого нагромадження даних в межах моделі. Відсутність деякої інформації по іншим філіалам призведе до зростання невизначеності в межах моделі.

Інформація рівня поточної версії системи буде співпадати з інформацією **рівня філіалу** за умови відсутності будь-яких змін в системі. При цьому, враховуються не лише зміни програмного (інсталяція нових програм, нових версій програм, перехід на ліцензійне ПЗ, віртуалізація ПЗ), а й апаратного забезпечення (придбання/втрата обладнання, зміни в топології мережі, зміна пропускної здатності каналів зв'язку, BYODpolicy). Інформація даного рівня використовується для визначення пріоритетних цілей для захисту.

Якщо система знаходиться на етапі розробки (робочої версії немає), то інформація рівня поточної версії буде складатися з:

1) даних про можливий саботаж (запобігання створенню системи);

2) даних про умисне відтермінування впровадження системи (без компрометації);

3) даних про компрометацію системи ще до її впровадження.

Рівень загрози порушника для поточної версії системи залежить від:

1) інсталяції та конфігурації системи;

2) паролів (або акаунтів) за замовчуванням;

3) періоду навчання персоналу (якщо додано новий функціонал);

4) періоду тестування (запуск системи на віртуальних машинах);

5) періоду зберігання попередньої версії (після деякого часу відкат до попередньої версії стає неможливим);

6) сумісності з попередніми версіями.

Так як будь-які зміни в межах поточної версії не допускаються, стороні захисту потрібно враховувати **кумулятивний** ефект деяких атак. Розглянемо наступний приклад: порушник проводить атаку, що компрометує окремий комп'ютер в нашій системі; сторона захисту передбачила подібний сценарій і прийняла рішення розподілити навантаження між рештою комп'ютерів; сторона захисту запланувала установку нового антивірусного ПЗ, що дозволить уникнути подібної атаки, наступного місяця; порушник повторює атаку, доки навантаження на ще не скомпрометовану частину системи не стане надмірним; подальший перерозподіл навантаження є недопустимим, до кінця місяця залишається декілька днів, а BYODpolicy не була узгоджена з керівництвом. В цьому прикладі кількісна нестача стала причиною поступового зростання загрози.

Так як для сторони захисту принциповою є незмінність системи протягом запланованого періоду функціонування, найбільшу загрозу становитимуть атаки, що порушують **Цілісність** та **Доступність**. У наведеному вище прикладі із поступовою компрометацією певного сегмента системи в початковий момент часу в системі була деяка надлишковість. Саме надлишковість ресурсів дозволила деякий час ігнорувати проблему. У випадку із порушенням **Конфіденційності**, сторона захисту може спробувати врятувати ще не скомпрометовану конфіденційну інформацію без внесення змін до системи (зміна паролів в межах поточної версії допустима, недопустимою є **зміна вимог** до довжини та складності паролів).

Модель порушника

Сторона захисту розробляє модель порушника відповідно до своїх вимог.

В межах даної роботи нас не цікавить обраний стороною захисту спосіб збору інформації. Інформація для моделі може бути отримана законно або незаконно, в повному обсязі або частково, мати довільний рівень достовірності (від явної дезінформації до точної на 100%), мати довільний рівень надлишковості(будь-які зайві дані, що будуть відкинуті при розробці моделі). Отримана інформація може бути формалізованою або не формалізованою. Приведення інформації до правильного формату також виходить за межі даної статті.

Для невеликих систем рівні організації, філіалу та поточної версії системи можуть бути об'єднані в один.

До інформації загального рівня відносять наступні дані:

1) наявність умислу/мотивації до проведення атаки;

2) тривалість атаки;

3) контроль за проведенням атаки;

4) контроль порушника за рівнем збитку, що завдає дана атака;

5) контроль порушника за середовищем, в якому здійснюється атака.

Так як наша система може стати об'єктом атаки випадково (без умислу), збитки від атаки не є гарантованими. Порушник може обійти всі впроваджені засоби захисту і не завдати шкоди, тому що:

а) порушник не зацікавлений в нанесенні збитку нам;

б) порушник зацікавлений в безперебійному функціонуванні нашої системи.

Результатом проведення атаки може стати установка backdoor в системі, який так і не буде використано. Можливим є і варіант установки логічної бомби, що ніколи не спрацює через задані порушником умови.

Інформація про тривалість атаки цікавить сторону захисту в першу чергу тоді, коли здійснюється атака на відмову в обслуговуванні. Порушник, що не зацікавлений в заподіянні збитків саме нашій системі, може через деякий час припинити атаку в даному напрямку. Порушник, що зацікавлений в безперебійному функціонуванні нашої системи, буде проводити лише атаки, що чинять мінімальний вплив на нашу систему (короткотермінові атаки).

В порушника може бути різний рівень контролю за проведенням атаки. Розповсюдження вірусів, мережевих хробаків та троянських програм складно контролювати. Троянські програми видають себе за корисне ПЗ. Порушник може лише обмежити кількість скачувань даної програми із сервера або самостійно розіслати дану програму жертвам. Після цього розповсюдження програми залежить вже від дій користувачів. Якщо порушник в явному виді не обмежить поширення шкідливого ПЗ, то єдиними обмеженнями будуть 1) рівень комп'ютерної грамотності користувачів та 2) системні вимоги до даного шкідливого ПЗ.

Мережеві хробаки можуть поширюватися за допомогою електронної пошти. Як і у випадку із троянськими програмами, порушник може розіслати мережевого хробака деякій множині користувачів, але після цього дане шкідливе ПЗ буде використовувати список адрес електронної пошти на вже інфікованих комп'ютерах. Віруси, за означенням, є типом програмного забезпечення, що має поширюватися самостійно. Навіть якщо у порушника є готова програма-антивірус, швидкість її поширення може бути нижчою, ніж швидкість поширення шкідливого ПЗ. Це означає, що в деяких випадках, навіть при бажанні, порушник не зможе зупинити/призупинити/відмінити атаку.

Аналогічно до контролю за тривалістю атаки важливими є і можливості порушника в плані контролю збитків. Якщо результатом атаки є шифрування всіх файлів на комп'ютері (програми ransomware), то порушник **може** знизити або повністю нівелювати збиток, передавши ключ для розшифрування (в даному випадку, ми розглядаємо ситуацію, коли наша система була атакована випадково і порушник намагається виправити ситуацію). Якщо результатом атаки є видалення даних, з багаторазовим пере записуванням відповідних секторів жорсткого диску псевдовипадковими послідовностями біт, то уникнути збитків буде практично неможливо.

Контроль за середовищем задає обмеження на проведення декількох одночасних атак. Інформація цього рівня дозволяє відповісти на питання:

1) «чи є у порушника можливість зупинити/призупинити/відмінити проведення атак іншими порушниками?»;

2) «чи зберігаються часові (інтервали часу, протягом яких порушник може доступатися до системи) та просторові (територія, з якої порушник може доступатися до системи) обмеження при проведенні атаки?».

До інформації рівня галузі відносяться дані для визначення пріоритетів порушників щодо вибору цілей для атаки. Так як на даному рівні збитки від проведеної успішної атаки є гарантованими, а імовірність активації загрози залежить від наявності інших систем, що вирішують подібні задачі, то важливими є дані про:

1) кількість альтернативних цілей (партнери, конкуренти):

1.1) розклад роботи для альтернативних цілей;

1.2) попередні успішні атаки проведені проти альтернативних цілей;

2) вагові коефіцієнти для цілей (частка інформації, що обробляється, частка клієнтів);

3) зв'язок між різними типами задач, які виконує дана система (чи є більш пріоритетним для порушника проведення атаки на спеціалізовану лише в 1 галузі систему? Чи буде зростати/зменшуватися пріоритет цілі від наявності додаткових задач?).

Інформація про альтернативні цілі є менш деталізованою, ніж інформація про систему, для якої розробляється модель порушника. Для сторони захисту в основному буде доступною інформація про приблизну кількість систем, що є подібними до даної. Від розкладу, за яким працює система,залежать:

– атаки на відмову в обслуговуванні (немає сенсу проводити подібну атаку, коли система не функціонує);

– атаки, що виконуються інсайдерами (хоча наслідки від атаки можуть проявитися в будь-який час, існує чіткий інтервал часу, протягом якого атаку потрібно розпочати).

Вагові коефіцієнти для цілей залежать від 1) частки вирішуваних задач та 2) виконання **важливих** задач. В другому випадку, пріоритет атаки на нашу систему зростає при надходженні конкретної задачі і знижується одразу після завершення даної задачі, незалежно від результату.

Для визначення пріоритету атаки на систему, що вирішує одразу декілька типів задач (декілька галузей), потрібно ввести метрику. Для деякого набору задач можна визначити порушників, що:

1) зацікавлені лише в 1 типі задач (будь-які інші задачі виключають цю підмножину порушників із моделі);

2) зацікавлені хоча б в 1 типі задач;

3) зацікавлені в деякій підмножині задач (строге включення);

4) зацікавлені в деяких аспектах роботи нашої системи (нестроге включення).

Для рівнів організації, філіалу та конкретної версії інформаційної системи відносять основні відомості про порушника, його ресурси, спільників, оцінку витрат порушника та прибутків у випадку проведення успішної атаки, сценарії атак.

Основною відмінністю для цих трьох рівнів є співвідношення множин атак та множин засобів захисту.

Для рівня організації для кожної атаки можна визначити декілька варіантів захисту (декілька множин засобів захисту, кожна з яких в достатній мірі захищає від атаки).

Для рівня філіалу одній множині атак відповідає лише одна множина засобів захисту. Представлена множина засобів захисту може бути більш ефективною у відношенні до одного виду атак та повністю пропускати інші атаки.

Для рівня поточної версії кожен засіб захисту має протистояти деякій множині атак (алгоритм шифрування має бути стійким до різних видів криптоаналізу, БД має бути захищена від різних типів SQL-ін'єкцій і т.д.).

Висновки

Основними відмінностями багаторівневої моделі порушника від решти моделей є поділ інформації на інформацію загального рівня та спеціалізовану інформацію. Подальший поділ спеціалізованої інформації визначатиме сумісність нашої моделі порушника з іншими моделями (або версіями моделі). Інформація загального рівня використовується для опису "випадкових" порушників, що проводять атаку без умислу. Модель передбачає можливість припинення атаки та відшкодування збитків в повному обсязі або частково з ініціативи порушника. Інформація рівня галузі використовується для обчислення імовірності **активації** загрози (зацікавленість порушника у проведенні атаки саме на нашу систему). Поділ решти моделі на рівні організації, філіалу та поточної версії зумовлений гнучкістю механізмів захисту. Для рівня організації сторона захисту має декілька варіантів подальшого розвитку системи і обирає найкращий із доступних. Для рівня філіалу набір засобів захисту є фіксованим і має гарантувати прийнятний рівень безпеки від фіксованого набору загроз. Рівень поточної версії є найбільш деталізованим. На даному рівні розглядають ефективність окремих механізмів захисту від множини загроз та/або послідовності атак (сценарії атак порушника).

Література

[1]. W. Liu, H. Tanaka, K. Matsuura, "Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms", *IPSZ Journal,* Vol. 48, no. 9, September 2007, pp. 3204-3218.

[2]. А. Архипов, "Применение рефлексивных моделей рисков для защиты информации в киберпространстве", *Захист інформації*, Т. 19, №3.

[3]. М. Мирошник, "Разработка средств защиты информации в распределенных компьютерных системах и сетях", *ІКСЗТ*, №1, 2015.

[4]. Ю. Хохлачова, "Політика інформаційної безпеки об'єкта", *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, №2(24), 2012.

УДК 004

Киреенко А. Модель нарушителя информационной безопасности с общей и специализированной информацией

Аннотация. *В этой статье приведены рекомендации по разработке модели нарушителя с информацией, которая отличается по уровню специализированности. Информацию более высокого (общего) уровня проще переносить из одной модели в другую (или из одной версии модели в следующую), в то время как специализированная информация используется для количественных оценок потерь от проведенной атаки. Разным уровням детализации информации о нарушителе соответствуют разные наборы средств защиты (отношение "много к одному" для уровня организации, "один к одному" для уровня филиала, "один ко многим" для уровня текущей версии системы). Разработанная в соответствии с данными рекомендациями модель нарушителя позволяет учитывать уровень контроля нарушителя за совершением атаки и приоритет выбора целей для атаки.*

Ключевые слова: *защита информации, модель нарушителя, сценарии атаки, угрозы, вероятность мотивации нарушителя, вероятность проведения успешной атаки, неоднородная информация, сходство атак.*

Kireienko O. Information security violator model with general and specialized information

Abstract. *User violator model is a collection of data that is used to analyze upcoming threats for our system. These models mostly focus on threats that are related to poorly-trained personnel, competitors that are willing to resort to industrial espionage and all sorts of hackers. User violator model can incorporate information about other non-human threats that can directly affect the actions of the violator. User violator model can contain information about threats for system itself and threats for information that is processed within the system or even a certain aspect of such information. While it is impossible to predict all attacks with absolute certainty, it is still convenient to have at least some insight into violator's plans. User violator model is also used for reaction planning and system/information recovery planning. Design of user violator models requires specific knowledge about both – the violators and the system. This work is dedicated to processing information about violator within the model in a way that will make it usable in other models. In this article recommendations for design of the violator model with information that differs by level of specialization are presented. Information of a higher (more generalized) level can be easily transferred to other models (or from current version of the model to the next one) whereas more specialized information is used for quantitative estimations of losses from performed attacks. Various levels of detailing of information about violator correspond to various sets of security mechanisms ("many to one" relation for the level of organization, "one to one" relation for the level of branch, "one to many" relation for the level of current version of the system). Violator model that is designed in accordance to these recommendations allows to account for violator's control over attack and attacks' target priority.*

Keywords: *information security, violator model, attack scenarios, threats, probability of violator's motivation, probability of successful attack, assorted information, similarity of attacks.*

Отримано 25 *лютого 2019 року*, затверджено редколегією *19 березня 2019 року*