© Kopytin Yu. Developing a model of information security risk assessment based on colored Petri net // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3, p. 293-299.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATION SECURITY MANAGEMENT

РОЗРОБКА МОДЕЛІ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ РОЗФАРБОВАНОЇ МЕРЕЖІ ПЕТРІ

Юрій Копитін

Відділ забезпечення захисту інформації КП «Обласний інформаційно-аналітичний центр», Україна

КОПИТІН Юрій Вікторович

Рік та місце народження: 1989 рік, м. Одеса, Україна.
Освіта: Одеська національна академія зв'язку, 2011 рік.
Посада: т.в.о. начальника відділу забезпечення захисту інформації КП «Обласний інформаційно-аналітичний центр» з 2013 року; аспірант ОНАЗ
Наукові інтереси: управління інформаційною безпекою, економічна безпека.
Публікації: 17 наукових статей та доповідей на міжнародних конференціях та семінарах, навчальний посібник.
E-mail: ykopytin@odessa.gov.ua

Анотація. *У статті проведено аналіз наявних моделей оцінки ризиків інформаційної безпеки на основі мереж Петрі за результатами якого визначено, що існуючі моделі оцінки ризиків недостатньо відображають структуру організації, що унеможливлює отримання цілісної картини відносно ризиків. Розроблено модель оцінки ризиків інформаційної безпеки на основі розфарбованої мережі Петрі та гіперграфів, яка дозволяє відслідковувати потенційну шкоду, нанесену порушниками внаслідок реалізації загроз через уразливості активів, та уникнені, використаними заходами й засобами захисту, наслідки від реалізації загроз за заданий проміжок часу. Запропоновано структуроване розбиття активів для збільшення точності їх ідентифікації. Результати моделювання ризиків за допомогою запропонованої моделі можуть бути практично використані на етапі оцінки ризиків інформаційної безпеки.*

Ключові слова: *інформаційна безпека, ризики інформаційної безпеки, оцінка ризиків, загрози, уразливість, атака, розфарбовані мережі Петрі, ймовірність, наслідки.*

Вступ

На сьогодні існує думка, що процеси оцінки та управління ризиками виступають фундаментом для побудови сталої та ефективної системи забезпечення інформаційної безпеки організації. В світі наявна значна кількість моделей, методів і методологій оцінки ризиків інформаційної безпеки, що використовують кількісні та якісні підходи для визначення оптимальних варіантів обробки ризиків, включаючи стандарти (ISO/IEC 27005, EBIOS, NIST SP800-30, OCTAVE та ін.) та спеціалізовані програмні продукти (CRAMM, Counter Measures, Гриф, РискМенеджер, Risk Watch та ін.). Однак існуючі моделі, методи та методології оцінки ризиків інформаційної безпеки дотепер чітко й однозначно не визначені і продовжують формуватися, тому вони по-різному розуміються, інтерпретуються і використовуються в публікаціях, документах та практичній діяльності. Практичне використання наявних на ресурсі [1] засобів автоматизації процесів оцінки ризиків показало, що вони характеризуються високою вартістю, значними трудовими витратами та складністю пропонованих рішень, що обмежує їх широке застосування й не дозволяє істотно спростити процедуру оцінки ризиків та підвищити точність одержуваних оцінок.

Аналіз існуючих досліджень

Одним із ефективних методів дослідження та оптимізації систем забезпечення інформаційної безпеки є імітація їх роботи за допомогою моделей, зокрема, на базі мереж Петрі. Основними перевагами від використання мереж Петрі у моделюванні ризиків інформаційної безпеки, так само, як і в моделюванні бізнес-процесів є: 1) процес має ясне та чітке відображення; 2) наочність побудови мережі, завдяки якій всі її визначення та алгоритми легко сприймаються; 3) можливість використання різних методів аналізу ризиків [2].

Моделюванню ризиків інформаційної безпеки з використанням мереж Петрі присвячено публікації Арькова П.О. [3], Мельник Г.В. [4], Пітера Стефенсона [5], Мет Генрі [6], Яхонтова І.В. [7] та інших. У зазначених роботах модельовано динаміку процесів автентифікації та ідентифікації

користувача, загрози та можливі реалізовані атаки, ймовірність реалізації загрози. Окрім цього, Пітер Стефенсон у роботі [5] висуває сумніви щодо доцільності проведення оцінки ризиків, прив'язаної до активів, аргументуючи це тим, що в середовищі, де використовуються десятки тисяч активів неможливо і недоцільно проводити повну інвентаризацію активів із встановленням взаємозв'язків між ними.

Моделі, наведені в зазначених роботах, не відображають всі активи, що унеможливлює отримання цілісної картини відносно ризиків організації. Для проведення комплексної оцінки ризиків необхідно ідентифікувати всі активи, їх уразливості, загрози, що можуть бути реалізовані, та наслідки. При цьому під час проведення оцінки ризиків слід чітко розподілити обов'язки і визначити хто, яку складову аналізує, оскільки, наприклад, ризики програмного забезпечення із закритим кодом може оцінити виключно розробник. Для спільного проведення оцінки відповідальними особами, слід розробити уніфіковану структуру описання кожного окремого ризику, на яку і зосереджено увагу у цій роботі.

Мета та завдання дослідження

Метою дослідження є розробка моделі оцінки ризиків інформаційної безпеки на основі розфарбованої мережі Петрі та гіперграфів, яка дозволить відслідкувати потенційну шкоду, нанесену порушниками внаслідок реалізації загроз через уразливості активів.

Основні завдання, спрямовані на досягнення поставленої мети:

- описати загальні засади функціонування організацій з позицій інформаційної безпеки;
- систематизувати активи організації для підвищення точності ідентифікації;
- сформувати структуру розфарбованої мережі Петрі, призначеної для оцінки ризиків інформаційної безпеки, з використанням програмних засобів.

Матеріали та методи дослідження

За основу розробки моделі оцінки ризиків на основі розфарбованої мережі Петрі покладено наступне бачення автора.

Організаціями для ведення ділових процесів використовуються активи. Розмежування доступу до активів реалізується за допомогою атрибутів доступу. Використання кожного активу, у свою чергу, пов'язане з уразливостями, які в подальшому можуть бути використані для реалізації загроз. Незалежно від роду діяльності організації завжди існують особи (порушники), які внаслідок своєї необізнаності або злого умислу, наносять їй шкоду. Серед множини активів завжди існують такі, до яких порушники мають санкціонований доступ, або наявні місця, в яких можливе неконтрольоване перебування порушників (наприклад, вулиця на яку виходять вікна приміщення, в якому обробляється інформація, що потребує захисту). Саме з зазначених активів та місць вони можуть розпочинати свої атаки. При цьому для використання уразливості порушники мають володіти певними навичками та мати у наявності ресурси для реалізації загроз, а також повинні витратити певний час на реалізацію атаки, зокрема час на виявлення певної уразливості активу та час на здійснення атаки з використанням уразливості. Зазначені атаки можуть повторюватися порушниками з певною періодичністю. Зазначимо, що через одну уразливість може бути реалізовано декілька різних загроз. Для забезпечення захисту від дії загроз організації використовують засоби та заходи захисту. Протидія одній загрозі може бути здійснена шляхом застосування більше ніж одного заходу або засобу захисту. При цьому не виключається ситуація, коли для протидії загрозі захисні механізми не застосовано.

У якості системи моделювання для побудови розфарбованої мережі Петрі використано програмний засіб CPN Tools. Розфарбовані мережі Петрі у системі моделювання CPN Tools являють собою комбінацію графа мережі Петрі та мови програмування CPN ML, використовуваної для опису атрибутів елементів. Фішка розфарбованої мережі Петрі являє собою елемент абстрактного типу даних, який зазвичай називається кольором [8].

На рис. 1 наведено фрагмент розробленої моделі на основі розфарбованої мережі Петрі, яка дозволяє відслідковувати потенційну шкоду, нанесену порушниками внаслідок реалізації загроз через уразливості активів, та уникнені, використаними заходами й засобами захисту, наслідки від реалізації загроз за заданий проміжок часу.

Нижче наведено лістинг команд, які необхідно реалізувати для функціонування моделі:

```
colset E = unit with e timed;
colset PERPETRATOR = record PER_id:STRING * PER_skill_l:INT * PER_capab:INT * PER_step:INT timed;
var per:PERPETRATOR;
colset ASSES = record ASS_id:STRING * PER_id:STRING * PER_skill_l:INT * PER_capab:INT * PER_step:INT * LIKELIHOOD:REAL timed;
var ass:ASSES;
colset VULNERABILITY = record ASS_id:STRING * VUL_id:STRING * PER_id:STRING * PER_skill_l:INT * PER_capab:INT * PER_step:INT * LIKELIHOOD:REAL timed;
var vuln:VULNERABILITY;
colset CONSEQUENCES = record ASS_id:STRING * VUL_id:STRING * TRE_id:STRING * PER_id:STRING * LIKELIHOOD:REAL * CONSEQ:REAL timed;
var con:CONSEQUENCES;
colset SM = record SM_id:STRING * ASS_id:STRING * VUL_id:STRING * TRE_id:STRING * PER_id:STRING * LIKELIHOOD:REAL * CONSEQ:REAL * PRICE:REAL timed;
var sm:SM;
fun init(ass_id, per_id, per_skill_l, per_capab, per_step, likelihood) = 1`{ASS_id = ass_id, PER_id = per_id, PER_skill_l = per_skill_l, PER_capab = per_capab, PER_step = per_step, LIKELIHOOD = likelihood};
(*input ass_id, likelihood*)
fun auth(ass)=1`ass;
```

fun search_vuln(vul_skill, search_time, ass_id, vul_id, per_id, per_skill_l, per_capab, per_step, likelihood)= if (per_skill_l >= vul_skill) then 1`{ASS_id = ass_id, VUL_id = vul_id, PER_id = per_id, PER_skill_l = per_skill_l, PER_capab = per_capab, PER_step = per_step, LIKELIHOOD = likelihood}@+search_time else empty;
*(*input vul_skill, search_time, vul_id*)*
*fun risk_now (have_sm, ass_id, vul_id, tre_id, per_id, per_step, likelihood_old:REAL, conseq:REAL, likelihood_new:REAL) = if have_sm=0 then if per_step=0 then 1`{ASS_id = ass_id, VUL_id = vul_id, TRE_id = tre_id, PER_id = per_id, LIKELIHOOD = likelihood_new, CONSEQ = conseq} else 1`{ASS_id = ass_id, VUL_id = vul_id, TRE_id = tre_id, PER_id = per_id, LIKELIHOOD = (likelihood_new * likelihood_old), CONSEQ = conseq} else empty; (*input have_sm,conseq,likelihood*).*

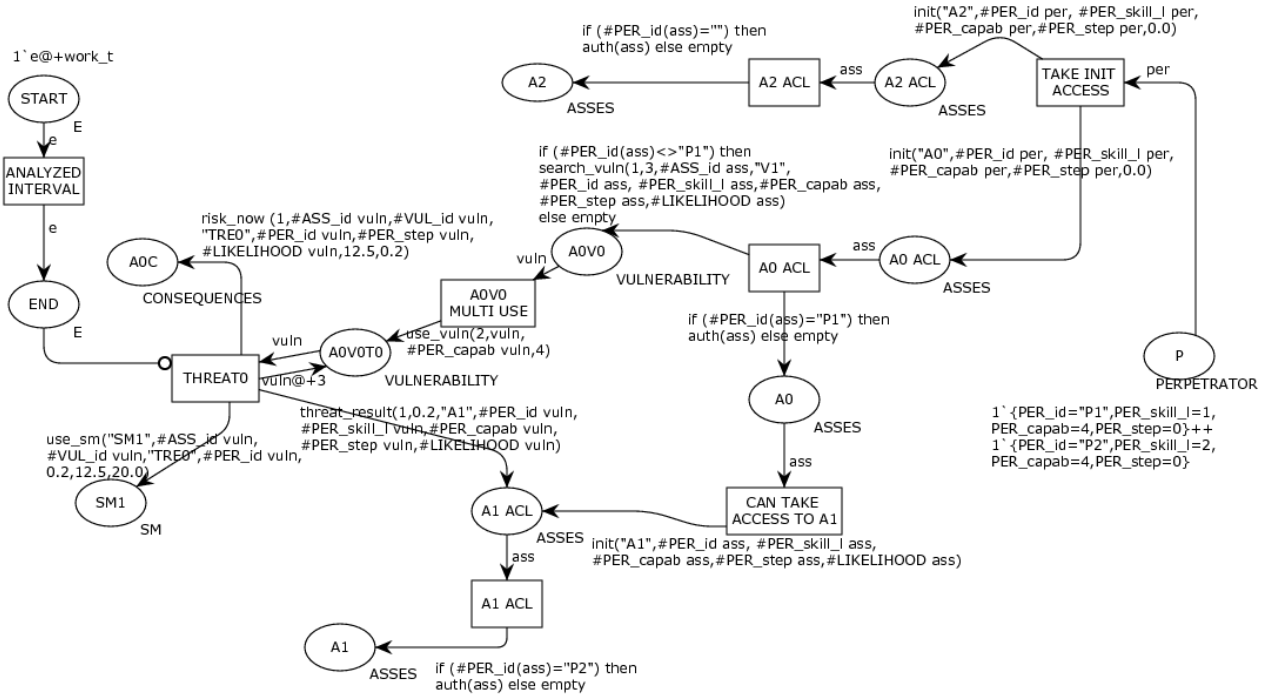

Рис. 1 Фрагмент моделі оцінки ризиків на основі розфарбованої мережі Петрі

fun use_vuln (vuln_capab ,vulner ,per_capab, time) = if (per_capab>=vuln_capab) then 1`vulner@+time else empty;
*fun threat_result(have_sm, likelihood_new:REAL, ass_id, per_id, per_skill_l, per_capab, per_step, likelihood_old:REAL) = if have_sm=0 then if (per_step=0) then 1`{ASS_id = ass_id, PER_id = per_id, PER_skill_l = per_skill_l, PER_capab = per_capab, PER_step = (per_step+1), LIKELIHOOD = likelihood_new} else 1`{ASS_id = ass_id, PER_id = per_id, PER_skill_l = per_skill_l, PER_capab = per_capab, PER_step = (per_step+1), LIKELIHOOD = (likelihood_new * likelihood_old)} else empty;(*input have_sm,likelihood,ass_id*)*
*fun use_sm(sm_id, ass_id, vul_id, tre_id, per_id, likelihood, conseq, price) = 1`{SM_id = sm_id, ASS_id = ass_id, VUL_id = vul_id, TRE_id = tre_id, PER_id = per_id, LIKELIHOOD = likelihood, CONSEQ = conseq, PRICE = price}; (*input sm_id,likelihood,conseq,price*)*
*val work_t=22;(*input work_time*).*

У загальному вигляді представлена модель складається із наступних позицій та переходів:

- позиція порушник *P*;
- позиції з відомостями про активи *A#id* (далі – позиція «актив»);
- позиції з атрибутами доступу до активів *A#id ACL* (далі – позиція «атрибут»);
- позиції з відомостями про уразливості *A#idV#id* (далі – позиція «уразливість»);
- позиції, які поєднують уразливості із загрозами *A#idV#idT#id* (далі – позиція «уразливість-загроза»);
- позиції з відомостями про наслідки *A#idC* (далі – позиція «наслідок»);
- позиції з відомостями про заходи (засоби) захисту *SM#id* (далі – позиція «захист»);
- позиції фіксування інтервалів часу *START* та *END*;
- перехід ініціалізації доступу порушників *TAKE INIT ACCESS*;
- переходи ініціалізації подальшого доступу *CAN TAKE ACCESS TO A#id* (далі – перехід «ініціалізація»);
- переходи санкціонування доступу до активів *A#id ACL* (далі – перехід «доступ»);
- переходи, які організовують множинне використання уразливості загрозами *V#id MULTI USE* (далі – перехід «розмножувач»);
- переходи, які описують дію загрози *THREAT#id* (далі – перехід «загроза»);
- перехід фіксування часу роботи *ANALYZED INTERVAL.*

Значення у позиції *P* складається з фішок типу *PERPETRATOR*, які містять початкові відомості про наявних порушників, зокрема: ідентифікатор порушника *PER_id*, коефіцієнт навичок порушника *PER_skill_l* (знаходиться у діапазоні від 1 до 5 та описує ступінь володіння відомостями про уразливість, вміння її знаходити та знання засобів та заходів, які необхідні для реалізації загрози), коефіцієнт наявних у порушника засобів для реалізації загрози через уразливість *PER_capab*

(знаходиться у діапазоні від 1 до 5), крок необхідний для реалізації загрози із застосуванням несанкціонованих дій *PER_step* (у позиції *P* дорівнює 0). Позиція *P* є єдиною точкою для введення відомостей про порушників. Зазначимо, що коефіцієнт навичок вищий, у випадку, коли від порушника для реалізації загрози через певну уразливість вимагаються більші знання. Коефіцієнт наявних у порушника засобів для реалізації загрози збільшується, у випадку необхідності використання більш складних та витратних заходів та засобів для нанесення атаки. Формування величини зазначених коефіцієнтів має стати темою окремого спеціалізованого дослідження

Позиції «актив» (на рис. 1 позиції *A0*, *A1*, *A2*) та позиції «атрибут» доступу (на рис. 1 позиції *A0 ACL, A1 ACL, A2 ACL*) складаються з фішок типу *ASSES*, які містять наступні відомості: назва (позначення) активу *ASS_id*, відомості про порушника, який отримав доступ до активу в поточний момент (*PER_id*, *PER_skill_l*, *PER_capab*, *PER_step*), а також ймовірність здійснення несанкціонованого доступу до активу *LIKELIHOOD* (задається в інтервалі від 0 до 1). Значення останнього параметра береться від попереднього активу, а для пограничних активів дорівнює 0. Під пограничними маються на увазі ті активи, до яких порушники всіх категорій мають вільний доступ (наприклад, комп'ютер у мережі Інтернет, з якого можна отримати доступ до порталу організації, або коридор, з якого можна увійти до приміщення організації, тощо).

Позиції «уразливість» (на рис. 1 позиція *A0V0*) складаються з фішок типу *VULNERABILITY*, які містять наступні відомості: назва (позначення) активу *ASS_id*, назва (позначення) уразливості *VUL_id*, відомості про порушника, який отримав доступ до уразливості в поточний момент (*PER_id, PER_skill_l, PER_capab, PER_step*), а також ймовірність здійснення несанкціонованого доступу через уразливість *LIKELIHOOD*.

Позиції «уразливість-загроза» (на рис. 1 позиція *A0V0T0*) складаються з фішок типу *VULNERABILITY*, які дублюють значення в позиції «уразливість».

Позиції «наслідок» (на рис. 1 позиція *A0C*) складаються з фішок типу *CONSEQUENCES,* які містять наступні відомості: назва (позначення) активу *ASS_id*, назва (позначення) використаної уразливості *VUL_id*, назва (позначення) реалізованої загрози *TRE_id*, відомості про порушника *PER_id*, ймовірність з якою реалізовано загрозу *LIKELIHOOD* та наслідки від її реалізації *CONSEQ* у гривнях або інших умовних одиницях.

Позиції «захист» (на рис. 1 позиція *SM1*) складаються з фішок типу SM, які містять наступні відомості: назву (позначення) засобу або заходу захисту *SM_id*, назва (позначення) активу *ASS_id*, назва (позначення) уразливості, яка закривається *VUL_id*, назва (позначення) загрози від якої здійснюється захист *TRE_id*, ймовірність з якою могла бути реалізована загроза *LIKELIHOOD*, потенційно уникнені негативні наслідки *CONSEQ*, вартість впровадження засобу (заходу) захисту *PRICE*.

Перехід *TAKE INIT ACCESS* використовується для демонстрації доступу порушників до пограничних активів, тобто місць, до яких порушник має вільний доступ та через які розпочинає процес отримання доступу до інших активів (наприклад, територія або приміщення, з яких можна розпочати реалізовувати локальні загрози, веб-сервер, через який можна розпочати реалізовувати віддалені загрози).

Переходи «атрибут» (на рис. 1 *A0 ACL*, *A1 ACL*, *A2 ACL*) або дозволяють доступ до активу та запускають функцію *auth,* або блокують та запускають функцію *search_vuln*.

Переходи «ініціалізація» (на рис. 1 *CAN TAKE ACCESS TO A1*) використовуються для демонстрації доступу порушників до активів з активу, до якого на попередньому кроці отримано санкціонований доступ порушником.

Переходи «розмножувач» (на рис. 1 *V0 MULTI USE*) використовуються для реалізації множинного застосування уразливостей загрозами.

Переходи «загроза» (на рис. 1 *THREAT1*) реалізовують перевірку: чи використовується засіб (захід) захисту, який протидіє реалізації певної загрози через певну уразливість. У випадку наявності захисних механізмів ініціюється функція *use_sm*, а у випадку їх відсутності – функції *threat_result* та *risk_now*.

Функція *init* забезпечує формування фішки типу *ASSES* для наступного на шляху просування активу. Функція *auth* забезпечує просування фішки типу *ASSES* до позиції, яка містить відомості про актив. Функція *search_vuln* забезпечує формування фішки типу *VULNERABILITY* у випадку, якщо порушник володіє навичками, необхідними для виявлення уразливості. Функція *use_vuln* забезпечує просування фішки типу VULNERABILITY у випадку, якщо порушник володіє засобами, необхідними для реалізації загроз через неї. Функція *threat_result* забезпечує формування фішки типу *ASSES* у випадку успішної реалізації загрози. Функція *risk_now* забезпечує формування фішки типу *CONSEQUENCES* у випадку успішної реалізації загрози. Функція *use_sm* забезпечує формування фішки типу *SM*. Параметри, які слід вводити для використання функцій у власній моделі, зазначено у лістингу.

У запропонованій моделі ймовірність реалізації послідовних загроз розраховується за формулою (1):

$$P_{total} = \prod_{i=1}^{n} P_i, \qquad (1)$$

де P - ймовірність реалізації однієї загрози.

Змінні *per, ass, vuln* використовується для просування фішок типу *PERPETRATOR, ASSES* та *VULNERABILITY* відповідно. Ребро зі змінною *vuln*, яке з'єднує позицію «уразливість-загроза» з переходом «загроза», забезпечує реалізацію процесу використання уразливості загрозою, враховуючи при цьому час, необхідний для її первинної та повторних реалізацій. При цьому, у випадку

можливості повторного використання загрози, від переходу «загроза» до позиції «уразливість-загроза» додається ребро із змінною *vuln* та часом затримки (на рис. 1 *vuln*@+*3*).

Для припинення процесу моделювання використовуються позиції *START* та *END*, перехід *ANALYZED INTERVAL*, змінна *work_t*, в якій задається часовий період моделювання, та інгібіторна дуга, яка кріпиться до кожного із переходів «загроза». В результаті спрацювання переходу *ANALYZED INTERVAL* через час *work_t* фішка із позиції *START* переходить у позицію *END*.

Запропонована автором модель дозволяє:

1. Ідентифікувати активи організації, які використовуються для виконання ділових процесів, у тому числі розташувати їх на схемі з урахуванням взаємного впливу.
2. Ідентифікувати потенційних порушників, у тому числі задати рівень їх навичок та можливостей.
3. Ідентифікувати уразливості активів та задати навички і час, які потрібні порушнику для виявлення уразливості активу.
4. Ідентифікувати загрози, які можуть бути реалізовані через наявні уразливості активів та задати необхідні можливості і час, які потрібні порушнику для первинної та повторної реалізації загрози через уразливість.
5. Ідентифікувати та задати наслідки від реалізації загроз.
6. Ідентифікувати та задати використовувані для протидії загрозам засоби і заходи захисту.
7. Задати атрибути доступу порушників до активів.
8. Задати пограничні активи, з яких порушник має початковий доступ до організації, та може розпочати реалізацію атак.
9. Задати досліджуваний інтервал часу у добах або в умовних одиницях.
10. Оцінити реалізовані за досліджуваний інтервал часу загрози.
11. Оцінити перелік дій, які слід виконати порушнику для реалізації певної загрози через певну уразливість.
12. Оцінити ймовірність реалізованих загроз з урахуванням переліку дій, які слід виконати порушнику.
13. Оцінити наслідки від реалізації загроз за досліджуваний інтервал часу.
14. Оцінити уникнені, за рахунок використання засобів або заходів захисту, збитки за досліджуваний інтервал часу.

Механізм роботи із моделлю наступний:

1. Провести ідентифікацію активів організації, які використовуються для виконання ділових процесів, шляхом нанесення на схему позицій «активи».

Для підвищення точності ідентифікації активів автором було проведено дослідження структури організації з позицій інформаційної безпеки за результатами якого встановлено, що активи організації зручно розбити на наступні складові: територіальне розміщення (віддалена зовнішня територія, зовнішня територія, яка прилягає до будівлі, кабінети, приміщення тощо); невід'ємні елементи приміщення (вікна, двері, розетки тощо); допоміжні технічні засоби (кондиціонери, опалення тощо); елементи фізичних процесів обробки та передачі інформації (сигнал у дротовій лінії зв'язку, WI-FI сигнал тощо); основні технічні засоби (комп'ютер, маршрутизатор, комутатор тощо); складові основних технічних засобів (материнська плата, оперативна пам'ять накопичувач на жорстких магнітних дисках тощо); базова підсистема вводу-виводу; контейнери системи віртуалізації; драйвери; директорії та файли; фонові процеси; процеси застосувань користувача; інтерфейси операційної системи (вікно консолі керування, редактор реєстру, диспетчер задач тощо); інтерфейси застосувань користувача (вікно браузера, інтерфейс користувача системи електронного документообігу тощо); бази даних та дані у таблицях баз даних; веб-застосунки; внутрішні мережеві порти; елементи логічної топології мережі (VLAN, DMZ тощо); зовнішні мережеві порти.

Для відображення на схемі взаємозв'язків між активами побудуємо гіперграф *H*, для описання якого введемо наступне: нехай *W* – кінцева непуста множина; *N* – певна родина підмножини множини *W*. Пара *(W,N)* називається гіперграфом *H=(W,N)* з множиною вершин *W={w}* та множиною ребер *N={n}*. Множину вершин *W* складають ідентифіковані активи організації. Множину ребер формують за наступним принципом: у випадку, якщо від функціонування активу не залежить функціонування інших активів, то ребро включає виключно вершину з нанесеним активом; у випадку, якщо від функціонування активу залежить функціонування інших активів, то ребро включає вершину з нанесеним активом та вершини із всіма залежними активами. Сформовані ребра гіперграфу *H* у мережі Петрі виступають у якості позицій «актив».

На рис. 2 наведено приклад гіперграфу, який відображає залежності між активами. Нехай вершина *w1* – це кабінет, *w2* – розетка, *w3* – комп'ютер. Ребро *n1={w1,w2,w3}* описує кабінет, у якому знаходиться розетка та комп'ютер. Ребро *n2={w2,w3}* означає, що комп'ютер підключено до розетки та залежить від її живлення. Ребро *n3={w3}* описує комп'ютер, який у наведеному прикладі не деталізовано.

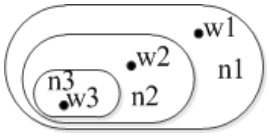

Рис. 2 Приклад гіперграфу, який відображає залежності між активами

2. Здійснити ідентифікацію потенційних порушників у позиції *P* шляхом задання фішок типу *PERPETRATOR*.
3. Задати атрибути доступу порушників до ідентифікованих активів шляхом нанесення позицій «атрибут», переходів «доступ» та задати перелік порушників, які мають доступ до активу, у операторі порівняння *if*.
4. Виконати ідентифікацію уразливостей активів за допомогою позицій «уразливість»

з'єднаних із переходом «доступ» та задати навички і час, які потрібні порушнику для виявлення уразливості активу у функції *search_vuln*.

5. Ідентифікувати загрози, які можуть бути реалізовані через наявні уразливості активів за допомогою позицій «уразливість-загроза» і переходів «загроза» та задати необхідні можливості і час, які потрібні порушнику для первинної реалізації загрози через уразливість у функції *use_vuln*. У випадку, якщо загроза може бути використана повторно, задати час, який потрібен для повторної реалізації загрози.

6. Ідентифікувати наслідки від реалізації загроз за допомогою відповідної позиції «наслідок», яку слід з'єднати із переходом «загроза». У випадку розповсюдження наслідків на різні активи від переходу «загроза» наносяться ребра до всіх необхідних позицій «наслідок». Окрім цього, від переходу «загроза» наносяться ребра до позицій «актив», до яких порушник може отримати доступ внаслідок реалізації загрози. В подальшому слід задати розмір та ймовірність настання збитків у функціях *risk_now, threat_result* та *use_sm*.

7. Ідентифікувати використовувані для протидії загрозам засоби і заходи захисту за допомогою позицій «захист», з'єднаних із відповідними переходами «загроза», та задати їх вартість у функції *use_sm*.

8. Задати пограничні активи, з яких порушник має початковий доступ до організації та може розпочати реалізацію атак, шляхом з'єднання переходу *TAKE INIT ACCESS* з позиціями «атрибут» відповідних активів.

9. У змінній *work_t* задати досліджуваний інтервал часу у добах або умовних одиницях.

10. Провести моделювання, за результатами якого можна виявити та оцінити реалізовані за досліджуваний інтервал часу загрози, ймовірність їх реалізації та наслідки, уникнені за допомогою заходів й засобів захисту негативні наслідки.

Обґрунтування моделі

Як зазначалось раніше, на сьогоднішній день порушник може реалізовувати загрози, як локально, так і віддалено. Прикладом локальних загроз є проникнення у приміщення організації з вулиці через уразливість, пов'язану із відсутністю решіток на вікнах або зняття інформації, перебуваючи на вулиці за рахунок побічних електромагнітних випромінювань внаслідок відсутності екранування; віддалених – проникнення у мережу організації шляхом надсилання листа із шкідливим кодом на загальновідому адресу електронної пошти або шляхом реалізації SQL-ін'єкції через відсутність перевірки даних, які вводяться користувачами на порталі організації тощо. Зазначена ситуація повністю реалізована в моделі завдяки переходу *TAKE INIT ACCESS*, який з'єднує позицію *P* з відповідними позиціями «атрибут». Зазначимо, що в описаних вище випадках, порушник може вільно перебувати на вулиці, знати загальнодоступну адресу скриньки електронної пошти, відвідувати веб-портал. Однак при цьому порушник не має доступу, як до приміщення організації, так і до мережі, окрім доступу до порталу. Запропонована модель дозволяє зазначити це у операторі порівняння *if* у дугах, які з'єднують перехід «доступ» з позиціями «актив» та «уразливість».

При цьому один актив може мати декілька уразливостей, наприклад, комп'ютер залежить від електроживлення, але не має джерела безперебійного живлення, а також боїться вологи, але знаходиться у вологому приміщені. Зазначене можна відобразити на схемі шляхом з'єднання ребрами переходу «Доступ» із відповідними позиціями «уразливість». Зазначена ситуація розповсюджується і на загрози, наслідки та заходи (засоби) захисту, та у повному обсязі реалізована в моделі.

Переваги моделі:

1. Модель дозволяє в межах одного рисунку ідентифікувати активи, атрибути доступу до активів, уразливості активів, порушників, загрози та заходи (засоби) захисту, вказати їх взаємний вплив, оцінити ймовірність виникнення негативних наслідків та їх величину, визначити дії, які порушник має виконати для реалізації загрози.

2. Модель дозволяє підвищити точність опису структури організації з точки зору інформаційної безпеки, що дозволяє провести якісний аналіз отриманих результатів та прийняти остаточне рішення щодо обробки ризиків.

Недоліки моделі:

1. Практичне застосування моделі неможливо без використання спеціально розроблених програмних засобів, які дозволятимуть наносити елементи на схему та задавати параметри в автоматизованому режимі, оскільки її складність зростає прямо пропорційно кількості нанесених активів та взаємозв'язків між ними. Під громіздкістю мається на увазі труднощі нанесення всіх позначень на схему вручну.

2. Можуть виникати труднощі із нанесенням заходів та засобів захисту, оскільки вони можуть розглядатися як актив, і мати уразливості, що можуть в подальшому бути використані порушниками під час реалізації загроз.

Зазначимо, що описані вище недоліки не впливають на роботу моделі, хоча й впливають на повноту відображення множини уразливостей, загроз, властивостей активів організації і, як наслідок, на точність отримуваних оцінок ризиків інформаційної безпеки. Зменшення впливу недоліків можливе за рахунок формалізації й автоматизації процесу підготовки вхідних даних, «інтелектуалізації» інтерфейсів моделі та підвищення вимог до кваліфікації оператора.

Висновки

У роботі запропоновано модель оцінки ризиків інформаційної безпеки на основі розфарбованої мережі Петрі та гіперграфів, яка дозволяє ретельно дослідити активи організації, визначити їх взаємний вплив, змоделювати загрози, які можуть бути реалізовані через уразливості активів, та наслідки від них, перевірити коректність впровадження заходів (засобів) захисту. Зазначена

модель може бути використана на практиці під час проведення ідентифікації ризиків та дослідження наслідків від реалізації загроз порушниками через уразливості активів організації за заданий інтервал часу, а результати моделювання за допомогою неї можуть бути використані під час обробки ризиків. Окрім цього модель може бути корисною в процесах розслідування інцидентів інформаційної безпеки, а також у навчальному процесі, оскільки вона дозволяє ретельно дослідити активи, зокрема виявити їх слабкості, змоделювати небезпечні події або дії, які можуть відбутися і в результаті яких може бути нанесена шкода, визначити заходи (засоби) протидії загрозам. Для її практичного застосування необхідно реалізувати програмний засіб, який дозволить автоматизувати процес нанесення компонентів на схему. В перспективу подальших досліджень входить модернізація розробленої мережі Петрі в ієрархічну, з урахуванням запропонованого розбиття активів, та формування модуля автоматизованого прийняття рішення стосовно обрання варіанту обробки ризиків.

Література

[1] Inventory of Risk Management / Risk Assessment Tools. — Режим доступу: http://rm-inv.enisa.europa.eu/tools

[2] Полещук Н.А. Анализ и планирование затрат предприятия на основе моделирования бизнес-процессов / Н.А. Полещук // Вестник Белорусского государственного экономического университета. — 2011. — N 1. — С. 60-65/

[3] Арьков П.А. Разработка комплекса моделей для выбора оптимальной системы защиты информации в информационной системе организации [Текст] : дис. … канд. техн. наук / П.А. Арьков. — Волгоград, 2009. — 185 с.

[4] Мельник Г.В. Моделювання системи управління інформаційними ризиками в корпоративній системі / Г.В. Мельник // Бізнес-інформ. — 2013. — № 9. — С. 95-99.

[5] Peter R. Stephenson A Formal Model for Information Risk Analysis Using Colored Petri Nets [Електронний ресурс]. — Режим доступу: URL: http://www.researchgate.net/publication/228909435_A_formal_model_for_information_risk_analysis_using_colored_petri_nets.

[6] Matt Henry Coupled Petri Nets for Computer Network Risk Analysis (Application to Process Control Networks) [Електронний ресурс] / Matt Henry, Ryan Layer, David Zaret. — Режим доступу: URL: http://www.sys.virginia.edu/risk/PDF%5CHENRY.pdf

[7] Яхонтов И.В. Анализ моделей систем защиты информации на основе модифицированных сетей Петри / И.В. Яхонтов // Методы и системы защиты информации, информационная безопасность. — 2012. — №3. — С. 57-65.

[8] Зайцев Д.А. Исследование эффективности технологии MPLS с помощью раскрашенных сетей Петри [Електронний ресурс] / Зайцев Д.А., Сакун А.Л. — Режим доступу: URL: http://teka.rulitm. ni/docs/2/1025/conv_1/filel.pdf

УДК 004.056 (045)

Копытин Ю.В. Разработка модели оценки рисков информационной безопасности на основе раскрашенной сети Петри

Аннотация. *В статье проведен анализ существующих моделей оценки рисков информационной безопасности, по результатам которого определено, что существующие модели оценки рисков недостаточно отражают структуру организации, что делает невозможным получение целостной картины относительно рисков. Разработана модель оценки рисков информационной безопасности на основе раскрашенной сети Петри и гиперграфов, которая позволяет отслеживать потенциальный вред, нанесенный нарушителями в результате реализации угроз через уязвимости активов, и предотвращенные, использованными мерами и средствами защиты, последствия реализации угроз за заданный промежуток времени. Предложено структурированное разбиение активов для повышения точности их идентификации. Результаты моделирования рисков с помощью предложенной модели могут быть использованы на практике на этапе оценки рисков информационной безопасности.*

Ключевые слова: *информационная безопасность, риски информационной безопасности, оценка рисков, угрозы, уязвимость, атака, раскрашенные сети Петри, вероятность, последствия.*

Kopytin Yu. Developing a model of information security risk assessment based on colored Petri net

Abstract. *The article analyzes the existing models of information security risk assessment as a result of which it is determined that the existing risk assessment models do not sufficiently reflects the structure of the organization, which makes it impossible to obtain a complete information about the risks. Developed a model of information security risk assessment based on colored Petri nets and hypergraphs, which allows you to track the potential harm caused by offenders as a result of threats through the vulnerability of assets and prevented the consequences of threats by used security measures and tools in the specified time. Structured partition of assets to improve the accuracy of their identification is proposed. The results of risk modeling using the proposed model can be used in practice in the phase of information security risks evaluation.*

Key words: *information security, information security risks, risk assessment, threat, vulnerability, attack, colored Petri nets, probability, consequences.*

Отримано *17 вересня 2014 року*, затверджено редколегією *9 жовтня 2014 року*