Применение теории гиперигр к анализу защищенности и поддержке принятия решений по реагированию на инциденты безопасности

Е. В. Федорченко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

{doynikova, ivkote}@comsec.spb.ru

И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

{doynikova, ivkote}@comsec.spb.ru

Boying WuGiven

Harbin Institute of Technology

mathwby@hit.edu.cn

Yin Li

Harbin Institute of Technology

liyin@hit.edu.cn

Аннотация. **К настоящему времени было предложено большое количество исследований по применению теории игр для моделирования взаимодействия кибератакующего и специалиста по информационной безопасности. Одной из проблем является тот факт, что в каждый момент времени кибератакующий и специалист по информационной безопасности не обладают точной информацией о стратегии противника, что порождает неопределенность при выборе собственной стратегии. В работе рассматривается применение теории гиперигр для учета данной неопределенности. При этом для определения возможных стратегий кибератакующего используется граф атак, в то время как для определения выигрыша при применении той или иной стратегии используется граф зависимостей между ресурсами информационной системы. Таким образом, результатом исследования является предложенный подход к анализу защищенности и поддержке принятия решений по реагированию на инциденты безопасности на основе теории гиперигр.**

Ключевые слова: информационная безопасность; теория игр; граф атак; граф зависимостей между ресурсами; гипериграа; поддержка принятия решений

I. Введение

Для анализа и реагирования на кибератаки активно применяются подходы на основе теории игр. Они позволяют имитировать поведение специалиста по информационной безопасности и кибератакующего и выбирать оптимальную стратегию для каждого.

Так, в работах [1, 2] теория игр применяется для оценки рисков информационной безопасности. В работе [3] рассматривается ее применение для мониторинга информационной безопасности. В ряде работ предлагаются подходы к применению теории игр для управления рисками информационной безопасности [4–11]. Ряд исследователей предлагает применять теорию игр для оценки уязвимостей [12].

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН

Существуют также обзоры по применению теории игр в кибербезопасности [13–18] и конфиденциальности персональных данных [19].

Тем не менее, существующие подходы имеют ряд недостатков, которые мешают как теоретическому развитию исследований в данной области, так и их практическому применению. В частности, существует проблема неопределенности, которая состоит в том, что в каждый момент времени атакующий и специалист по информационной безопасности обладают как определенной, так и неопределенной информацией о системе и действиях противника, т. е. неполной и некорректной информацией. Это отражается на выборе стратегии. Для учета неопределенности в данном исследовании предлагается подход на основе теории гиперигр. Для отображения возможных стратегий атакующего и специалиста по информационной безопасности в виде последовательностей действий предлагается использовать графы атак. Для определения выигрыша при применении той или иной стратегии предлагается применять графы зависимостей между ресурсами системы, позволяющие отобразить распространение ущерба. Таким образом, новизна предлагаемого подхода состоит в формализации этапов определения модели поведения специалиста по информационной безопасности и кибератакующего с использованием теории гиперигр путем применения ряда взаимосвязанных аналитических моделей, в том числе графов атак и графов зависимостей между ресурсами информационной системы.

II. Предлагаемый подход

Предлагаемый подход предполагает определение модели поведения специалиста по информационной безопасности и кибератакующего с использованием теории гиперигр, которая будет применяться для оптимизации стратегий игроков. Для определения данной модели необходимо: (1) определить ресурсы, которые необходимо защитить, или модель информационной системы; (2) назначить игроков, в том

числе ту информацию, которой они обладают, в данном случае, модель кибератакующего и специалиста по информационной безопасности; (3) определить стратегии, в данном случае модель атак и защиты; (4) задать цели атакующего и специалиста по информационной безопасности; (5) определить игру; (6) найти оптимальную стратегию [20].

Рассмотрим подробнее этапы определения модели поведения специалиста по информационной безопасности и кибератакующего с использованием теории гиперигр.

A. Определение модели информационной системы

Определим модель информационной системы следующим образом: $IS = (H, L, LT)$, где H – множество хостов, L – множество связей между хостами, LT – тип связи между хостами. H определяется доступными ресурсами $R = (T, Cr)$, где T – тип ресурса, выделяются активы, порты и программно-аппаратное обеспечение, $Cr = [Cr(c)\ Cr(i)\ Cr(a)]$ – критичность ресурса с точки зрения конфиденциальности $Cr(c)$, целостности $Cr(i)$ и доступности $Cr(a)$. Для определения ущерба в случае успешной реализации стратегии кибератакующего используется граф зависимостей между ресурсами системы, позволяющий отобразить распространение ущерба. Определим его следующим образом [21]:

$$ADG=(A, D, \varepsilon),$$

где A – множество узлов графа или ресурсов;

$D = (a_i, a_j, W)$, $D \subseteq A \times A$ – множество связей графа или зависимостей между ресурсами, $a_i, a_j \in A$, $a_j \in Des(a_i)$, $Des(a_i)$ – множество потомков a_i, от свойств безопасности которых напрямую зависят свойства безопасности a_i, W – весовая матрица, определяющая степень зависимости свойств безопасности предка от свойств безопасности потомка;

$\varepsilon = (D, td)$ – тип зависимости между ресурсами, $td \in$ {И, ИЛИ}, зависимость типа «И» означает, что для сохранения свойств безопасности ресурса необходимо сохранение свойств безопасности нескольких ресурсов потомков, зависимость типа «ИЛИ» – для сохранения свойств безопасности ресурса необходимо сохранение свойств безопасности одного из ресурсов потомков, выделяются структурные и функциональные зависимости.

Итоговая критичность ресурсов системы по параметрам конфиденциальности, целостности и доступности $E\_Cr = [E\_Cr(c)\ E\_Cr(i)\ E\_Cr(a)]$ определяется путем обхода графа зависимостей между ресурсами системы, начиная с ресурсов, у которых нет предков [22]: $E\_Cr = Cr + W \cdot Cr_{Des(a)}$, где $Cr_{Des(a)}$ – критичность зависимых ресурсов системы.

Для определения ущерба от реализации стратегии кибератакующего по параметрам конфиденциальности $Impact(c)$, целостности $Impact(i)$ и доступности $Impact(a)$, учитывается критичность атакуемого ресурса и разрушительность атакующего действия:

$$[Impact(c)\ Impact(i)\ Impact(a)] = \\ = [E\_Cr(c)\ E\_Cr(i)\ E\_Cr(a)] \times [cImpact\ iImpact\ aImpact],$$

где $cImpact$, $iImpact$, $aImpact$ – индексы системы оценивания уязвимостей CVSS [27], влияние на конфиденциальность, целостность и доступность, соответственно.

Итоговый ущерб определяется суммированием ущерба по трем свойствам.

B. Определение модели кибератакующего и специалиста по информационной безопасности

Модель кибератакующего задается следующим образом: $A = (H, Sk, AG)$, где H – хосты, к которым кибератакующий имеет доступ до проведения кибератак, AG – цели атакующего, Sk = {None, Low, Medium, High} – уровень навыков атакующего.

Модель специалиста по информационной безопасности задается следующим образом: $D = (H, R, DG)$, где H – хосты, для которых доступны средства защиты от кибератак, DG – цели специалиста по информационной безопасности, R – ресурсы, доступные для защиты.

C. Моделирование стратегий

Под стратегией кибератакующего будем понимать последовательность атакующих действий, позволяющих реализовать киберугрозу для ресурса информационной системы. Для моделирования стратегий кибератакующего предлагается использовать графы атак. Зададим граф атак следующим образом [23, 24]: $G = (S, L, Pc)$, где S – множество узлов графа, соответствующих атакующим действиям, $S = (H, V, Sc, St, Pr)$, H задает атакованный хост (включает описание ресурсов хоста), $V = (P, R, I)$ – использованную уязвимость, R и I определяют результат атакующего действия, $P = (AT, R)$ – необходимые условия для возможности выполнения атакующего действия, AT – необходимый тип доступа (AT = {remote, local), R – необходимые привилегии, Sc определяет атаку, направленную на сбор информации о хосте, St – состояние атакующего действия (St = {True, False}), Pr – вероятность того, что атакующее действие находится в состоянии St ($Pr \in [0,1]$);

L – множество связей между атакующими действиями ($L \subseteq S \times S$);

Pc – дискретные локальные распределения условных вероятностей.

На основе графа атак определим вероятности успешной реализации каждой стратегии – безусловные вероятности компрометации узлов графа [25]:

$$Pr(S_1, \ldots, S_n) = \prod^n_{i=1} Pc(S_i|Pa(S_i)),$$

где S_i – i-й узел графа;

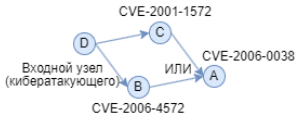
$Pa(S_i)$ – все предки узла S_i, узел м.б. связан с узлами предками отношением «И» – для успешной компрометации узла S_i необходимо, чтобы все предки узла $Pa(S_i)$ были скомпрометированы (цепочка последовательно связанных узлов графа), или отношением «ИЛИ» – необходимо скомпрометировать хотя бы один из предков узла (узлы графа, находящиеся на одном уровне);

$Pc(S_i|Pa(S_i))$ – функция локального распределения условной вероятности, т. е. вероятности компрометации узла S_i с учетом различных комбинаций состояний его предков $Pa(S_i)$.

Для определения распределений условной вероятности всех узлов применяется обратный обход графа атак в глубину начиная с узлов, не имеющих потомков, и заканчивая узлами, доступными кибератакующему, с учетом типов связей между узлами предками. В случае связей типа «И» между узлами предками [26]: $Pc(S_i|Pa(S_i)) = 0$, если $\exists\, S_i \in Pa(S_i)|\, S_i = 0$, $Pc(S_i|Pa(S_i)) = p(S_i)$, иначе, где $p(S_i)$ – локальная вероятность компрометации узла S_i. В случае связей типа «ИЛИ» между узлами предками [26]: $Pc(S_i|Pa(S_i)) = 0$, если $\forall\, S_i \in Pa(S_i)|\, S_i = 0$, $Pc(S_i|Pa(S_i)) = p(S_i)$, иначе.

Для определения локальной вероятности $p(S_i)$ компрометации узла S_i используются индексы CVSS [27]: $p(S_i) = 2 \times AccessVector \times AccessComplexity \times \times Authentication$, если S_i является входным узлом графа, доступным кибератакующему, и $p(S_i) = 2 \times \times AccessComplexity \times Authentication$, иначе, где *AccessVector* – вектор доступа к уязвимости по CVSS; *AccessComplexity* – сложность доступа к уязвимости по CVSS; *Authentication* – требуемая аутентификация по CVSS.

Пример вычисления локальной, условной и безусловной вероятностей для фрагмента графа атакующих действий приведен на рис. 1.



$p(D)$	1
$p(B)$	0.99968
$p(C)$	0.99968
$p(A)$	0.85888

	$Pc(C\|D)$	$Pc(C\|\neg D)$
D	0.99968	0.00032
¬D	0	1

	$Pc(B\|D)$	$Pc(B\|\neg D)$
D	0.99968	0.00032
¬D	0	1

		$Pc(A\|B,C)$	$Pc(\neg A\|B,C)$
B	C	0.85888	0.14112
B	¬C	0.85888	0.14112
¬B	C	0.85888	0.14112
¬B	¬C	0	1

$Pr(D)$	1
$Pr(B)$	0.99968
$Pr(C)$	0.99968
$Pr(A)$	0.86

Рис. 1. Пример вычисления вероятностей для фрагмента графа

D. Задание целей атакующего и специалиста по информационной безопасности

Определим цели кибератакующего *AG* как максимизацию выигрыша кибератакующего B_A: $AG = \max B_A$, т.е. максимизацию риска информационной безопасности R для целевой системы при минимизации затраченных ресурсов кибератакующего C_A: $AG = (\max R, \min C_A)$. Цели специалиста по информационной безопасности определим как максимизацию его выигрыша B_D: $DG = \max B_D$, т.е. минимизацию риска информационной безопасности R для целевой системы при условии минимизации затраченных ресурсов специалиста по информационной безопасности C_D: $DG = (\max R, \min C_D)$. Риск информационной безопасности определяется как комбинация вероятности успешной реализации атаки и ущерба в результате успешной реализации атаки. Для определения вероятности успешной реализации атаки будем использовать графы атак, отображающие возможные стратегии атакующего. Для определения ущерба будем использовать графы зависимостей между ресурсами системы, позволяющие отобразить распространение ущерба.

E. Гипериграа

Отличие гипериграы от игры состоит в том, что в случае игры игроки имеют одинаковые представления о целях друг друга. В случае гипериграы один или более игроков могут иметь некорректное представление о целях соперников и таким образом играть в несколько разных игр. В [28] отмечено, что для случая двух игроков, кибератакующего и специалиста по информационной безопасности, наиболее естественной является гипериграа второго уровня HG^2, когда каждый из двух игроков может иметь некорректное представление о стратегии противника:

$$HG^2 = \{HG^1{}_1, HG^1{}_2, \ldots, HG^1{}_n\},$$

$$\forall i \in n, \exists\, i, j \in n : HG^1{}_i \neq HG^1{}_j,$$

где $HG^1{}_i = [HG^0{}_{1i}, \ldots, HG^0{}_i, \ldots, HG^0{}_{ni}]$;
$HG^0{}_{i,j} = [V_{1ji}, V_{2ji}, \ldots, V_{kji}, \ldots, V_{nji}]$, $\forall k \in n_{ji}$, $\forall j \in n_i$, $\forall i \in n$;
V_{kji} – представление i-го игрока о том как j-й игрок воспринимает цели игрока k, $i \neq j \neq k$, $i, j, k \in n$;
V_{ji} – цель i-го игрока с точки зрения j-го игрока,
V_j – реальная цель i-го игрока, которая может быть достигнута путем реализации стратегии S_i,
n – количество игроков.

Тогда гипериграа по информационной безопасности для двух игроков, кибератакующего и специалиста по информационной безопасности, будет определена следующим образом [28]:

$$HG^2 = \{HG^1{}_A, HG^1{}_D\},$$

где $HG^1{}_A = \{G_{AA}, G_{DA}\}$ – гипериграа первого уровня атакующего, $HG^1{}_D = \{G_{AD}, G_{DD}\}$ – гипериграа первого уровня специалиста по информационной безопасности;
G_{AA} – игра атакующего с точки зрения атакующего,
G_{DA} – игра специалиста по информационной безопасности с точки зрения атакующего, G_{AD} – игра атакующего с точки зрения специалиста по информационной безопасности, G_{DD} – игра специалиста по информационной безопасности с точки зрения специалиста по информационной безопасности.

Цели специалиста по информационной безопасности и атакующего определяются на основе графа атак и графа распространения ущерба.

F. Определение оптимальной стратегии

Для нахождения равновесия гипериграы второго уровня необходимо вначале проанализировать каждую игру и затем каждую гипериграу первого уровня, т.е. алгоритм поиска оптимальной стратегии для HG^2 можно определить следующим образом [28]:

1. Анализ целей игр G_{AA}, G_{AD}, G_{DA} и G_D для поиска точек равновесия.

2. Анализ гипериграы $HG^1{}_A$ с учетом равновесия игры кибератакующего G_{AA} и игры специалиста по информационной безопасности G_{DA} с точки зрения кибератакующего для поиска точек равновесия гипериграы $E_A = E_{AA} \cap E_{DA}$.

3. Анализ гипериграы $HG^1{}_D$ с учетом равновесия игры кибератакующего G_{AD} и игры специалиста по информационной безопасности G_{DD} с точки зрения

специалиста по информационной безопасности для поиска точек равновесия гиперигры $E_D = E_{AD} \cap E_{DD}$.

4. Анализ гиперигры HG^2 для поиска точек равновесия $E = E_{AA} \cap E_{DD}$.

III. Заключение

Подходы на основе теории игр позволяют анализировать поведение кибератакующего с целью выбора оптимальной стратегии поведения специалиста по информационной безопасности, но имеют ряд недостатков. В частности, существует проблема неопределенности, которая состоит в том, что в каждый момент времени атакующий и специалист по информационной безопасности не обладают полной и точной информацией о действиях противника, что отражается на выборе стратегии. В рамках данной работы предлагается использовать подход на основе теории гиперигр для учета этой неопределенности. В работе рассмотрены 6 этапов подхода, которые необходимы для построения модели анализа защищенности и поддержки принятия решений по реагированию на основе теории гиперигр, а именно, предложена модель информационной системы, которая позволяет определить ресурсы, которые необходимо защитить; определены модели игроков, а именно, модель кибератакующего и специалиста по информационной безопасности, определены стратегии кибератакующего на основе графа атак, определены цели атакующего и специалиста по информационной безопасности с использованием графа атак и графа зависимостей между ресурсами, определена модель поведения кибератакующего и специалиста по информационной безопасности в виде гиперигры второго уровня и представлен алгоритм определения оптимальной стратегии. Необходимо отметить, что существуют и другие проблемы, в том числе, проблема ресурсов, требуемых для выбора оптимальной стратегии в реальном времени, а также проблема одновременной реализации множества атак и выделения этих атак. Эти проблемы планируется рассмотреть в будущих исследованиях.

Список литературы

[1] Rajbhandari L., Snekkenes E. Utilizing Game Theory for Security Risk Assessment // Game Theory for Security and Risk Management. 2018. С. 3-19.

[2] Xu Y.L., Ling L.W. Study on Risk Assessment of Network Security Based on Game Theory // Advanced Materials Research. Trans Tech Publications, Ltd., 2011. Т. 181–182. С. 799-803.

[3] Game Theory with Learning for Cyber Security Monitoring / Chung K., Kamhoua C.A., Kwiat K.A., Kalbarczyk Z.T., Iyer R.K. // High Assurance Systems Engineering (HASE): Тез. докл. IEEE 17th International Symposium, Orlando, FL, USA, 2016. С. 1-8.

[4] Rass S., Schauer S. Game Theory for Security and Risk Management: From Theory to Practice. Springer International Publishing, 2018.

[5] Breitenbucher A. Gaming The System: A Game Theoretic Approach To Risk Management And Cybersecurity // Senior Independent Study Theses. 2022. Т. 9910.

[6] Zarreh A., Saygin C., Wan H., Lee Y., Bracho A. A game theory based cybersecurity assessment model for advanced manufacturing systems // Procedia Manufacturing. 2018. Т. 26. С. 1255-1264.

[7] Zarreh A., Wan H., Lee Y., Saygin C., Janahi R.A. Risk Assessment for Cyber Security of Manufacturing Systems: A Game Theory Approach // Procedia Manufacturing. 2019. Т. 38. С. 605-612.

[8] Game Theoretical Model for Cybersecurity Risk Assessment of Industrial Control Systems / Nassar M., Khoury J., Erradi A., Bou-Harb, E. // New Technologies, Mobility and Security (NTMS): Тез. докл. 11th IFIP International Conference, 2021.

[9] Wu C.-K. A game theory approach for risk analysis and security force deployment against multiple coordinated attacks // Environmental Research. 2021. Т. 194. С. 110737.

[10] Musman S., Turner A. A game theoretic approach to cyber security risk management // The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology. 2017. Т. 15, вып. 2. С. 127-146.

[11] A network security assessment model based on attack-defense game theory / Wang B., Cai J., Zhang S., Li J. // Computer Application and System Modeling: Тез. докл. International Conference, 2010.

[12] A Game Theoretic Framework for Network Vulnerability Assessment and Mitigation / Gueye A., Marbukh V. // Decision and Game Theory for Security: Тез. докл. International Conference, 2012. Т. 7638.

[13] A Survey of Game Theory as Applied to Network Security / Roy S., Ellis C., Shiva S., Dasgupta D., Shandilya V., Wu Q. // System Sciences: Тез. докл. 43rd Hawaii International Conference, 2010, Honolulu, HI, USA. С. 1-10.

[14] Pham V.H. Applications of Game Theory in Information Security. 2015.

[15] Akinwumi D., Iwasokun G., Alese B., Oluwadare S. A review of game theory approach to cyber security risk management // Nigerian Journal of Technology, 2018. Т. 36. С. 1271.

[16] Tavafoghi H., Ouyang Y., Teneketzis D., Wellman M.P. Game Theoretic Approaches to Cyber Security: Challenges, Results, and Open Problems / Jajodia, S., Cybenko, G., Liu, P., Wang, C., Wellman, M. (eds) // Adversarial and Uncertain Reasoning for Adaptive Cyber Defense. Lecture Notes in Computer Science. Springer, Cham, 2019. Т. 11830.

[17] Chukwudi A., Eze U., Ikerionwu C. Game Theory Basics and Its Application in Cyber Security // Advances in Wireless Communications and Networks. 2017. Т. 3. С. 45-49.

[18] Liang X., Xiao Y. Game Theory for Network Security // Communications Surveys & Tutorials. IEEE, 2013. Т. 15. С 472-486.

[19] Do C.T., Tran N.H., Hong C., Kamhoua C.A., Kwiat K.A., Blasch E., Iyengar S.S. Game Theory for Cyber Security and Privacy // ACM Computing Surveys. 2017. Т. 50, вып. 2. С. 1-37.

[20] Rajbhandari L., Snekkenes E. Utilizing Game Theory for Security Risk Assessment// Game Theory for Security and Risk Management. 2018. С. 3-19.

[21] Cost evaluation for intrusion response using dependency graphs / Kheir N., Debar H., Cuppens-Boulahia N., Cuppens F., Viinikka J. // Network and Service Security: Тез. докл. International Conference, Paris, 24-26 June 2009 / IEEE, 2009. С. 1-6.

[22] Дойникова Е.В., Котенко И.В. Оценивание защищенности и выбор контрмер для управления кибербезопасностью. Москва: РАН, 2021. 184 с.

[23] Kotenko I., Doynikova E. Selection of countermeasures against network attacks based on dynamical calculation of security metrics // Journal of Defense Modeling and Simulation. 2018. Т.15, вып. 2. С. 181-204.

[24] Дойникова Е.В., Котенко И.В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер // Труды СПИИРАН. 2018. Т. 57, вып. 2. С. 211-240.

[25] Poolsappasit N., Dewri R., Ray I. Dynamic security risk management using Bayesian attack graphs // IEEE Transactions on Dependable and Security Computing. 2012. Т. 9, вып. 1. С. 61-74.

[26] Measuring network security using dynamic Bayesian network / Frigault M., Wang L., Singhal A., Jajodia S. // Quality of Protection: Тез. докл. ACM Workshop, 2008.

[27] Mell P., Scarforne K., Romanosky S. A Complete Guide to the Common Vulnerability Scoring System (CVSS) Version 2.0. 2007.

[28] Imamverdiyev. Y. A Hypergame Model for Information Security // International journal of information security science. Т. 3, вып. 1.