УДК 004.056.5; 004.72 DOI: 10.30748/soivt.2018.54.12

І.С. Добринін, М.П. Борова

Харківський національний університет радіоелектроніки, Харків

ОПТИМІЗАЦІЯ ВИБОРУ ВАРІАНТУ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД АТАК ПРИ АНТАГОНІСТИЧНІЙ ГРІ

У статті запропоновано використання математичного апарату теорії ігор для обґрунтування прийняття рішення щодо вибору варіанту побудови системи інформаційного захисту корпоративної мережі. Показано, що задача, яка розглядається, може бути віднесена до дуельної гри з нульовою сумою, гравцями якої є адміністратор мережі та потенційний зловмисник. Окреслені шляхи вирішення подібного класу задач з акцентом на ітеративний метод Брауна-Робінсон. Запропонований підхід щодо вибору засобів захисту базується на математичному апараті теорії ігор та дозволяє приймати рішення в умовах обмеженого бюджету підприємства.

Ключові слова: *інформаційна безпека, загроза, антагоністична гра, вразливість, актив.*

Вступ

Постановка проблеми у загальному вигляді. Впровадження систем менеджменту інформаційної безпеки стає все більш важливим явищем, що впливає на успіх компаній на сьогоднішній день. При розглядані питання захисту інформаційної системи, необхідно розуміти, що систему не можна вважати безпечною лише тому, що було куплено та встановлено певні засоби захисту, якими б популярними вони не вважались. Окремі посилання на необхідність використання певних засобів захисту містяться у існуючих стандартах з інформаційної безпеки, наприклад у лінійці стандартів ISO/IEC 27000 [1]. Проте, у відомих стандартах не надаються рішення (рекомендації) щодо оптимізації вибору доцільного варіанту побудови систем захисту.

Крім того, деякі підходи до побудови системи захисту корпоративних мереж (КМ) передбачають побудову цієї системи на основі певних шаблонів використання засобів захисту. У цьому випадку завдання визначення переліку та оптимізації вартості обраних заходів і засобів захисту не ставиться. Таким чином, відсутність суворої методики обґрунтування вибору конкретних заходів і способів захисту може привести до неоптимальності, а іноді навіть до неспроможності обраного набору компонентів системи захисту виконувати свої функції.

Саме тому, вирішення питань, пов'язаних з алгоритмізацією дій спрямованих на прийняття рішення щодо вибору ефективних засобів захисту, є актуальною науково-практичною задачею.

Аналіз досліджень і публікацій. На сьогоднішній день питанням обґрунтування варіанту побудови систем захисту інформації приділяється достатня увага. Так, в [2] пропонується оптимізацію вибору засобів захисту проводити за критерієм «переваги вибору», що обчислюється як сумарний показник експертних оцінок і додаткових показників, зважених коефіцієнтами важливості, за кожним видом засобів захисту окремо – захисту від несанкціонованого доступу, міжмережним екранам, антивірусним засобам. Окремі підходи [3] передбачають будувати на основі метода аналізу ієрархії (MAI) Т. Сааті парето-оптимальну множину, з якої адміністратор може вибрати рішення користуючись експертними знаннями. Окрім того, MAI покладено в основу результатів наведених у [4]. Деякі інші роботи, наприклад [5], акцентовані на визначенні оцінки ефективності інвестицій в засоби захисту, за результатами яких приймається рішення щодо обрання варіанту захисту.

У роботах [6–7] показано, що для вирішення задач побудови систем захисту інформації може використовуватися теорія ігор.

Мета статті: обґрунтування підходу щодо вибору ефективних засобів захисту корпоративної мережі за критерієм мінімізації потенційних збитків від атак при дуельній грі з нульовою сумою в умовах обмеженого бюджету підприємства.

Виклад основного матеріалу

Конкретизуємо постановку завдання.

Нехай існує корпоративна мережа, захист якої передбачає використання різноманітного програмного та апаратного обладнання (засобів захисту), перелік та комбінація яких обираються адміністратором мережі з урахуванням обмеженого кошторису щодо їх придбання та експлуатації.

Корпоративна мережа має вразливості, що можуть призвести до порушення цілісності, конфіденційності та доступності інформації, внаслідок чого компанії завдається матеріальна шкода зловмисником. Будемо вважати, що загрози корпоративній мережі відомі апріорі (наприклад, за допомогою статистики та бібліотек атак CAPEC, ISACA, OWASP Top Ten та ін.).

Завдання полягає у наступному: при апріорі заданому векторі загроз обрати оптимальну комбіна-

цію засобів захисту корпоративної мережі від локальних та мережних загроз за критерієм мінімізації потенційних збитків від атак при обмеженому бюджеті організації.

Враховуючи становище із загрозами інформаційній безпеці та різноманіттям засобів захисту КМ, а також враховуючи ймовірнісно-грошові потоки, описану проблему можна вирішити за допомогою математичного апарату теорії ігор, який дозволяє [8]: сформувати задачу щодо захисту КМ в математичному вигляді, що дозволяє скористатися розробленими критеріями знаходження оптимальних стратегій захисту; оцінити витрати на забезпечення безпеки інформаційного ресурсу, збитки від успішної реалізації атаки та з урахуванням цих даних прийняти оптимальне рішення; обрати набір засобів ефективного захисту інформації.

Дослідження взаємовідносин між зловмисником та адміністратором (особою, яка приймає рішення) передбачає, що вони є гравцями в деякій грі, де кожна сторона робить свої кроки, вибираючи ту чи іншу стратегію поведінки, прагнучи оптимально забезпечити свій інтерес. Метою гри є пошук оптимальної стратегії поведінки як по відношенню до адміністратора, так і по відношенню до зловмисника, адже обидві сторони, як правило, намагаються звести до мінімуму свої невдачі.

На першому кроці для пошуку найбільш ефективних стратегій захисту інформаційних ресурсів необхідно провести математичну дуельну бінарну гру двох сторін, однією з яких будемо вважати систему захисту інформації, а з іншого – можливі атаки зловмисників. Оскільки метою даної роботи є визначення адміністратором безпеки оптимальної стратегії захисту, а цілі зловмисників, що атакують, по суті, не важливі, то можна вважати, що зловмисник захоплений бажанням завдати якомога більшої шкоди системі.

В якості стратегій адміністратора безпеки будемо розуміти рядки $S_i (i = 1,...,n)$ матриці гри, а в якості стратегій зловмисника – її стовпці $A_j (j = 1,...,m)$. До стратегій адміністратора можна віднести різні засоби захисту інформації та всі можливі комбінації один з одним, до стратегій зловмисника – різноманітні види локальних та мережних атак. Елементами матриці є ймовірності успішної реалізації атаки зловмисником p_{ij} за умови, що використовується одна з можливих комбінацій засобів захисту. Зауважимо, що ймовірності розставляються з урахуванням того, що використовуються не лише нові, а й вже існуючі засоби захисту інформації (за умови, що такі існують).

Припускається, що елементи комбінації засобів захисту незалежні один від одного, тобто робота або несправність одного з них ніяк не впливає на інший. Тому, виходячи з теореми [9], що ймовірність поєднання декількох незалежних подій дорівнює добутку ймовірностей цих подій, ймовірність успішної реалізації атаки при використанні комбінацій різних засобів захисту буде виглядати наступним чином:

$$P(AB) = P(A) \cdot P(B).$$

При такому припущенні отримуємо матрицю для гри двох осіб, варіант якої надано у табл. 1, де рядок S_0 надає ймовірність успішної реалізації атаки при використанні поточних (апріорі використовуваних) засобів захисту інформації.

Таблиця 1

Початкова матриця для гри двох осіб

	A_1	A_2	…	A_m
S_0	p_{01}	p_{02}	…	p_{0m}
S_1	p_{11}	p_{12}	…	p_{1m}
S_2	p_{21}	p_{22}	…	p_{2m}
...	...	...	…	...
S_n	p_{n1}	p_{n2}	…	p_{nm}
S_{1+2}	$p_{11} \cdot p_{21}$	$p_{12} \cdot p_{22}$		$p_{1m} \cdot p_{2m}$
…	…	…	…	…

Передбачається, що також відомі ймовірності проведення кожного типу атак $p_j^{(A)}$, значення яких залежить від статистичних даних, а також оцінені вартість кожного із засобів захисту $X_i (i = 1,...,n)$ та розмір передбачуваного збитку від реалізації певної атаки $Y_j (j = 1,...,m)$.

Акцентуємо, що процесу оцінювання ймовірностей реалізації загроз і вразливостей необхідно приділяти особливу увагу. Виконання даного етапу можна доручити як групі внутрішніх співробітників, так і спеціальним експертам. Також необхідно використовувати не тільки експертні дані самої організації, але й враховувати статистику загроз, яку проводять аналітичні агентства з інформаційної безпеки.

Для того, щоб приймати рішення про доцільність впровадження певної системи захисту інформації, потрібно враховувати потенційні збитки при успішній реалізації атаки, потенційний виграш при впровадженні системи захисту інформації, а також реальні витрати на впровадження та підтримку працездатності системи захисту інформації.

Отже, наступним кроком є вирішення цієї задачі за допомогою фінансово-економічної оцінки інвестицій, а саме показника повернення інвестицій (ROI) для кожного елементу табл. 1, який розраховується наступним чином:

$$ROI_{ij} = benefits_{ij} - costs_i,$$

де $benefits_{ij}$ – оцінка тієї користі (тобто очікуваного зниження потенційних збитків), яку приносить

впровадження i-ї системи захисту інформації при реалізації j-ї атаки;

$costs_i$ – витрати на впровадження та підтримку працездатності i-ї системи захисту інформації.

Оцінка користі розраховується за допомогою наступної формули:

$$benefits_{ij} = R_{0j} - R_{ij},$$

де R_{0j} – потенційні збитки при реалізації j-ї атаки при використанні поточних (апріорі використовуваних) засобів захисту інформації;

R_{ij} – потенційні збитки при реалізації j-ї атаки з впровадженням i-ї системи захисту інформації.

Потенційні збитки розраховуються з урахуванням ймовірності успішної реалізації атаки зловмисником p_{ij} (за умови, що атака буде проведена зі стовідсотковою ймовірністю), ймовірності проведення певного типу атак $p_j^{(A)}$, а також розміру передбачуваного збитку від реалізації певної атаки Y_j. На основі цього отримаємо вираз:

$$R_{ij} = p_{ij} \cdot p_j^{(A)} \cdot Y_j.$$

Витрати на впровадження та підтримку працездатності i-ї системи захисту інформації дорівнюють X_i.

Отже, фінальна версія формули для розрахунку ROI виглядає наступним чином:

$$ROI_{ij} = p_{0j} \cdot p_j^{(A)} \cdot Y_j - p_{ij} \cdot p_j^{(A)} \cdot Y_j - X_i = \\ = (p_{0j} - p_{ij}) \cdot p_i^{(A)} \cdot Y_j - X_i$$

Розрахувавши ROI для кожного елементу початкової матриці, отримаємо нову матрицю гри (див. табл. 2), де елементи матриці є кількісною характеристикою вигоди впровадження конкретної системи захисту відносно певного типу атаки.

Таблиця 2

Матриця гри двох осіб після перерахування ROI для кожного елементу початкової матриці

	A_1	A_2	…	A_m
S_0	ROI_{01}	ROI_{02}	…	ROI_{0m}
S_1	ROI_{11}	ROI_{12}	…	ROI_{1m}
S_2	ROI_{21}	ROI_{22}	…	ROI_{2m}
...	...	...	…	...
S_n	ROI_{n1}	ROI_{n2}	…	ROI_{nm}

Наступним кроком є розв'язання отриманої матриці. Проведені дослідження показали, що для наближеного рішення таких матриць може використовуватися ітеративний метод Брауна-Робінсон [10].

Враховуючи вищевикладене, для існуючої матриці розглянемо нескінченний процес повторення даної гри, при якому кожен з гравців на кожному кроці передбачає, що противник вибере змішану стратегію, яка визначається частотами появ чистих стратегій на попередніх кроках, а сам обирає чисту стратегію, що забезпечує найкращий результат при даному припущенні.

Припустимо, що вже зроблено k повторень гри, в яких перший гравець вибирав чисті стратегії $i_1,...,i_k$, а другий – $j_1,...,j_k$. Тоді, відповідно до вищесказаного, перший гравець вибере на $(k+1)$-му кроці стратегію i_{k+1} з наступної умови:

$$\frac{1}{k}\sum_{\nu=1}^{k} a_{i_{k+1}j_\nu} = \max_{1\le i\le n} \frac{1}{k}\sum_{\nu=1}^{k} a_{ij_\nu} = \nu_1(k),$$

де k – номер кроку; a_{ij} – елемент матриці гри; n – кількість стратегій першого гравця; ν – ціна гри.

А другий гравець обере стратегію j_{k+1} із умови:

$$\frac{1}{k}\sum_{\nu=1}^{k} a_{i_\nu j_{k+1}} = \max_{1\le j\le m} \frac{1}{k}\sum_{\nu=1}^{k} a_{i_\nu j} = \nu_2(k),$$

де k – номер кроку; a_{ij} – елемент матриці гри; m – кількість стратегій другого гравця; ν – ціна гри.

У випадку, якщо стратегій, які відповідають відповідним умовам, декілька, гравець вибирає будь-яку з них.

Таким чином [10], ітеративний процес збігається до істинного значення гри, тобто:

$$\lim_{k\to\infty} \nu_1(k) = \lim_{k\to\infty} \nu_2(k) = \nu.$$

Воно означає, що уявні платежі $\nu_1(k)$ та $\nu_2(k)$ прагнуть до справжньої ціни гри ν, що в нашому випадку є оптимальною стратегією побудови системи захисту інформації.

Слід зазначити, що, у відповідності з [10], збіжність цього ітеративного методу повільна, але сам метод є достатньо простим і в певній мірі відображає набуття гравцями досвіду в результаті багатьох повторень конфліктної ситуації.

Очікувати від методу Брауна-Робінсон оцінок, близьких до дійсних значень, можна лише при великій кількості ітерацій [10]. Для цього потрібна реалізація автоматизації процесу обчислень, тому в рамках цієї роботи, авторами була розроблена програма, яка на основі початкових даних формує всі можливі комбінації засобів захисту інформації, розраховує показники повернення інвестицій для кожного елементу і знаходить оптимальну стратегію за допомогою вищеназваного методу.

Висновки

У роботі було вирішено задачу, яка полягала в розробці методики вибору доцільного варіанту побудови системи інформаційного захисту від атак за

критерієм мінімізації потенційних збитків від атак при дуельній грі з нульовою сумою.

Результати роботи можуть бути корисними для керівників підприємств чи відповідальних осіб в різноманітних корпоративних мережах компаній, які прагнуть вибрати ефективні та дієві засоби захисту інформації в умовах обмеженого бюджету.

Подальшим розвитком роботи мають бути дослідження, спрямовані на використання ігор з природою, що можуть бути доцільними за умов виникнення невідомих та неочікуваних вразливостей.

Список літератури

1. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements, ISO website [Електронний ресурс] – Режим доступу до ресурсу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.

2. Прокушева А.П. Моделирование и оптимизация выбора средств программно-аппаратной защиты информации с точки зрения экономической и технической целесообразности / А.П. Прокушева, Я.Е. Прокушев // Информация и безопасность. – 2012. – №1. – С. 55-60.

3. Хазлиев В.Н. Методика выбора оптимального набора средств программно-аппаратной защиты информации / В.Н. Хазлиев, Д.И. Кузьмин // Физико-математические науки и информационные технологии: проблемы и тенденции развития: сб. ст. по матер. VIII междунар. науч.-практ. конф. – 2012. – № 8.

4. Шматко О.В. Багатокритеріальний вибір систем захисту інформації за допомогою нечітких парних порівнянь альтернатив / О.В. Шматко, Є.В. Сичев // Системи обробки інформації. – 2011. – № 3. – С. 161-164.

5. Евсеев С.П. Оценка эффективности инвестиций в безопасность организаций банковского сектора на основе синергетической модели угроз / С.П. Евсеев // Системи обробки інформації. – 2017. – № 2. – С. 88-94. https://doi.org/10.30748/soi.2017.148.17.

6. Павлов І.М. Аналіз підходів оцінки ефективності математичних моделей при проектуванні систем захисту інформації / І.М. Павлов, С.В. Толюпа // Сучасний захист інформації. – 2014. – № 3. – С. 36-44.

7. Павлов І.М. Аналіз підходів моделювання процесів прийняття рішень при проектуванні систем захисту інформації / І.М. Павлов, С.В. Толюпа // Сучасний захист інформації. – 2014. – № 2. – С. 59-68.

8. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах / Л.Л. Гончарова, А.Д. Возненко, О.І. Стасюк, Ю.О. Коваль. – К., 2013. – 435 с.

9. Корн Г.А. Справочник по математике для научных работников и инженеров / Г.А. Корн, Т.М. Корн. – М.: Наука, 1974. – 832 с.

10. Лабскер Л.Г. Игровые методы в управлении экономикой и бизнесом / Л.Г. Лабскер, Л.О. Бабешко. – М.: Дело, 2001. – 464 с.

11. Толюпа С.В. Підходи до проектування та оцінки ефективності системи захисту інформації в автоматизованих системах обробки та передачі даних / С.В. Толюпа, О.М. Іванова, І.О. Демченко // Сучасний захист інформації. – 2013. – № 1. – С. 25-30.

12. Рубан И.В. Исследование удаленных атак на распределительно вычислительные сети / И.В. Рубан, С.С. Серов // Системи обробки інформації. – 2013. – № 5. – С. 118-120.

13. Чукляев И.И. Игровая модель обоснования применения средств комплексной защиты информационных ресурсов иерархической информационно-управляющей системы / И.И. Чукляев // T-Comm: Телекоммуникации и транспорт. – 2015. – № 2. – С. 64-68.

14. Толюпа С.В. Методика оцінки комплексної системи захисту інформації на об'єкті інформаційної діяльності / С.В. Толюпа, І.В. Борисов // Сучасний захист інформації. – 2013. – № 2. – С. 43-49.

References

1. "ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements", *ISO website,* www.iso.org/ iso/home/store/catalogue_tc/catalogue_detail.htm?csnumbe r=54534.

2. Prokusheva, A.P. and Prokushev, Ya.E. (2012), "Modelirovanie i optimizatsiya vyibora sredstv programmno-apparatnoy zaschityi informatsii s tochki zreniya ekonomicheskoy i tehnicheskoy tselesoobraznosti" [Modeling and optimization of the choice of software and hardware protection of information in terms of economic and technical feasibility], *Information and security*, No. 1, pp. 55-60.

3. Hazliev, V.N. and Kuzmin, D.I. (2012), "Metodika vyibora optimalnogo nabora sredstv programmno-apparatnoy zaschityi informatsii" [Method of choosing the optimal set of software and hardware protection of information], *Physical and mathematical sciences and information technology: problems and development tendencies: collection of articles on the materials of the VIII International Scientific and Practical. Conference*, No 8.

4. Shmatko, O.V. and Sychev, Y.V. (2011), "Bahatokryterialnyi vybir system zakhystu informatsii za dopomohoiu nechitkykh parnykh porivnian alternatyv" [Multiobjective choice of systems of protection of the information by means of indistinct pair comparisons of alternatives], *Information processing systems*, No 3, pp. 161-164.

5. Evseev, S.P. (2017), "Otsenka effektivnosti investitsiy v bezopasnost organizatsiy bankovskogo sektora na osnove sinergeticheskoy modeli ugroz" [Assessment of investments efficiency in security of banking sector organizations based on synergetic model], *Information processing systems*, No. 2, pp. 88-94. https://doi.org/10.30748/soi.2017.148.17.

6. Pavlov, I.M. and Toliupa, S.V. (2014), "Analiz pidkhodiv otsinky efektyvnosti matematychnykh modelei pry proektuvanni system zakhystu informatsii" [Analysis of approaches to assessing the effectiveness of mathematical models in the design of information security systems], *Modern information security*, No 3, pp. 36-44.

7. Pavlov, I.M. and Toliupa, S.V. (2014), "Analiz pidkhodiv modeliuvannia protsesiv pryiniattia rishen pry proektuvanni system zakhystu informatsii" [Analysis of approaches to modeling decision-making processes in the design of information security systems], *Modern information security*, No. 2, pp. 59-68.

8. Honcharova, L.L., Voznenko, A.D., Stasiuk, O.I and Koval, Yu.O. (2013), "*Osnovy zakhystu informatsii v telekomunikatsiinykh ta kompiuternykh merezhakh*" [*Fundamentals of information protection in telecommunication and computer networks*], Kyiv, 435 p.

9. Korn, G.A. and Korn, T.M. (1974), "S*pravochnik po matematike dlya nauchnyih rabotnikov i inzhenerov*" [*Handbook on mathematics for the Scientific workers and engineers*], Nauka, Moscow, 832 p.

10. Labsker, L.G. and Babeshko, L.O. (2001), "*Igrovyie metodyi v upravlenii ekonomikoy i biznesom*" [*Game techniques in the management of economics and business*], Delo, Moscow, 464 p.

11. Toliupa, S.V., Ivanova, O.M. and Demchenko, I.O. (2013), "Pidkhody do proektuvannia ta otsinky efektyvnosti systemy zakhystu informatsii v avtomatyzovanykh systemakh obrobky ta peredachi danykh" [Approaches to the design and evaluation of the effectiveness of the information security system in automated data processing and transmission systems], *Modern information security*, No. 1, pp. 25-30.

12. Ruban, I.V. and Serov, S.S. (2013), "Issledovanie udalennyih atak na raspredelitelno vyichislitelnyie seti" [Study of an attack against the computer network of distribution], *Information processing systems*, No 5, pp. 118-120.

13. Chuklyaev, I.I. (2015), "Igrovaya model obosnovaniya primeneniya sredstv kompleksnoy zaschityi informatsionnyih resursov ierarhicheskoy informatsionno-upravlyayuschey sistemyi" [The game model of the rationale for the use of integrated information resource protection for a hierarchical information management system], *T-Comm: Telecommunications and transport*, No. 2, pp. 64-68.

14. Toliupa, S.V. and Borysov, S.V. (2013), "Metodyka otsinky kompleksnoi systemy zakhystu informatsii na obiekti informatsiinoi diialnosti" [Methods of assessing the complex information security systems on information activities of the facility], *Modern information security*, No. 2, pp. 43-49.

Надійшла до редколегії 3.04.2018
Схвалена до друку 22.05.2018

Відомості про авторів:

Добринін Ігор Станіславович
кандидат технічних наук доцент
доцент кафедри Харківського національного
університету радіоелектроніки,
Харків, Україна
https://orcid.org/0000-0001-8910-2609

Борова Марина Петрівна
студентка магістратури Харківського національного
університету радіоелектроніки,
Харків, Україна
https://orcid.org/0000-0002-1174-1061

Information about the authors:

Ihor Dobrynin
Candidate of Technical Sciences Associate Professor
Senior Lecturer of Kharkiv National University
of Radio Electronics,
Kharkiv, Ukraine
https://orcid.org/0000-0001-8910-2609

Maryna Borova
Graduate Student of Kharkiv National University
of Radio Electronics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-1174-1061

ОПТИМИЗАЦИЯ ВЫБОРА ВАРИАНТА ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ АТАК ПРИ АНТАГОНИСТИЧЕСКОЙ ИГРЕ

И.С. Добрынин, М.П. Борова

В статье предложено использование математического аппарата теории игр для обоснования принятия решения по выбору варианта построения системы информационной защиты корпоративной сети. Показано, что рассматриваемая задача может быть отнесена к дуэльной игре с нулевой суммой, игроками которой является администратор и потенциальный злоумышленник. Указанны пути решения подобного класса задач с акцентом на итеративный метод Брауна-Робинсон. Предложенный подход к выбору средств защиты базируется на математическом аппарате теории игр и позволяет принимать решения в условиях ограниченного бюджета предприятия.

Ключевые слова: *информационная безопасность, антагонистическая игра, угроза, уязвимость, актив.*

OPTIMIZING THE CHOICE OF A VARIANT OF CONSTRUCTING A SYSTEM FOR PROTECTING INFORMATION FROM ATTACKS IN AN ANTAGONISTIC GAME

I. Dobrynin, M. Borova

The article proposes a variant of using the mathematical apparatus of game theory to justify making a decision on the choice of a variant of constructing an information protection system for a corporate network.

The initial data for the task were:

– a typical corporate network, the protection of which presupposes the availability of various software and hardware equipment (devices of protection), the list and combination of which are selected by the network administrator, taking into account the limited budget for their acquisition and exploitation;

– list of typical corporate network threats that can lead to violation of integrity, confidentiality and availability of information

It is shown that the problem under consideration can be referred to a zero-sum dueling game, of which the player is an administrator and a potential attacker. It is considered that the attacker uses vulnerabilities to damage the company. The task of the administrator is to choose effective devices of protecting the corporate network, provided that the company's limited budget.

The ways of solving this class of problems are indicated. It is shown that for the given initial data, the Brown-Robinson iterative method can be applied.

Thus, in this article, the task was solved that was to develop a method for choosing an appropriate variant of constructing a system for protecting information from attacks by the criterion of minimizing the potential damage from attacks with a zero-sum duel game.

The results of the work can be useful for business executives or responsible persons in various corporate networks of companies who are trying to choose effective and useful software and hardware (protection devices) to protect information in view of a limited budget.

Keywords: *information security, threat, antagonistic game, vulnerability, asset.*