УДК 004.056 Вестник УрФО № 2(52) / 2024, с. 37–45

Котельников Н. Д., Афанасьева М. В., Баранкова И. И.

DOI: 10.14529/secur240204

ПРИМЕНЕНИЕ ДВУСТОРОННЕЙ СИГНАЛЬНОЙ ИГРЫ В ТЕХНОЛОГИЯХ DECEPTION ДЛЯ ВЫБОРА ОПТИМАЛЬНОЙ СТРАТЕГИИ ЗАЩИТЫ

Все чаще для борьбы с сетевыми атаками сотрудники кибербезопасности прибегают к использованию методов киберобмана (deception). Технология deception, использующая ложные данные для привлечения злоумышленников, позволяет выявлять попытки нежелательного доступа к сети и предотвратить атаку на ранних стадиях.

Несмотря на эффективность средств киберобмана, их развертывание является сложным и дорогостоящим. Необходимо понимать, при каких условиях использование данных технологий будет наиболее целесообразным.

Использование теории игр помогает анализировать стратегии злоумышленников и разрабатывать наиболее эффективные методы защиты. Одним из способов определения оптимальной стратегии защиты является динамическая игра с неполной информацией (сигнальная игра), где один из игроков (атакующий или защитник) является отправителем сигнала, а второй игрок – получателем.

В статье предлагается расширить сигнальную игру до двусторонней: рассмотреть действия, как злоумышленников, так и сотрудников кибербезопасности, рассчитать возможные их выгоды от осуществления атаки и реализации системы защиты. Данная модель позволит оценить необходимость использования средств киберобмана и выбрать наиболее эффективную стратегию защиты.

Ключевые слова: *информационная безопасность, сетевая атака, технология обмана, стратегия защиты, теория игр, сигнальная игра.*

Kotelnikov N. D., Afanasyeva M. V., Barankova I. I.

APPLICATION OF TWO-SIDED SIGNALING GAME IN DECEPTION TECHNOLOGIES TO SELECT THE OPTIMAL DEFENSE STRATEGY

Increasingly, cybersecurity officials are turning to deception techniques to combat network attacks. Deception, which uses false data to lure attackers, can detect unwanted network access attempts and prevent attacks early on.

Despite the effectiveness of cyber deception tools, their deploying is complex and costly. It is important to understand under what conditions the use of these technologies will make the most sense.

The use of game theory helps analyze attacker strategies and develop the most effective defense techniques. One way to determine the optimal defense strategy is a dynamic game with incomplete information (signaling game), where one of the players (attacker or defender) is the sender of the signal, and the second player is the receiver.

The paper proposes to extend the signaling game to a two-sided game: consider the actions of both attackers and cybersecurity personnel, and calculate their possible benefits from the attack and the implementation of the defense systemThis model will allow us to assess the need to use cyber defenses and choose the most effective defense strategy.

Keywords: *information security, network attack, deception technology, defence strategy, game theory, signal game.*

Введение

Рост киберпреступности наносит огромный денежный и репутационный ущерб предприятия, нивелируя выгоду от использования информационных систем.

В целях защиты от компьютерных вторжений и обнаружения кибератак на ранних этапах была разработана технология deception, позволяющая запутать или ввести в заблуждение злоумышленников. В основе deception лежат техники обмана злоумышленников путем применения ловушек, приманок и других способов запутывания преступников [1]. Цель защитников заключается в предоставлении ложной информации, способной вывести атакующего «из игры». Злоумышленникам приходится тратить дополнительные ресурсы (например, время и деньги). Защитники же получают оперативную информацию о проникновении и реагируют на любые действия атакующего[2].

Развертывание средств обмана является дорогостоящей и сложной задачей: злоумышленник может найти и обойти ловушку или использовать её против защищающегося. Необходимо, чтобы ловушка обеспечивала максимальную вероятность того, что злоумышленник совершит атаку на неё, а не на реальную систему. Необходимо выбрать правильную последовательность защитных мер, предсказав действия атакующего, предотвратить процесс атаки и максимизировать свою выгоду. Методы теории игр помогают проверить и повысить эффективность технологий обмана. В [3] затрагивается вопрос выбора стратегии ложной информационный системы на основе модели теории игр. В работе учитываются показатели игроков и все возможные ограничения.

В [4] разработана биматричная игровая модель взаимодействия информационной системы с агрессивной внешней средой. Отдельно в работе рассматриваются возможные варианты трансформации базовой статической биматричной модели в динамическую игру с неполной информацией.

Применение сигнальных игр в deception технологиях обсуждалось в [5]. В работе [6] сигнальная игра была рассмотрена со стороны атакующего и защитника, с целью определения возможных действий нарушителя.

В статье предложен метод определения оптимальной стратегии, основанный на двусторонней сигнальной игре, который позволит эффективно применять технологии киберобмана в качестве защиты сети. Существенным отличием от методов [5,6] является то, что игра, предложенная в статье, является многоэтапной и двусторонней, где атакующий и защитник, наблюдая за действиями конкурента, постоянно изменяют стратегию своих действий.

Сигнальная игра

Сигнальная игра характеризуются неполнотой информации о соперниках. Злоумышленник не может понять, насколько защищенной является система, которую он собирается атаковать. Защитник не имеет представления о нападающем, о его возможностях и о технологиях, доступных ему.

Иными словами, в задачах подобного рода выбор решения зависит от состояний объективной действительности, называемой в модели «природой». [7]. Природа не является разумным игроком, она не заинтересована в выигрыше. Её роль – задать начальные условия, по которым будет проходить игра в дальнейшем. В сигнальной игре Природа наделяет отправителя сигнала типом θ. Знание о типе соперника дает информацию о его стратегиях и выигрышах, позволяет выбрать оптимальное решение. Однако Получатель сигнала не знает о типе отправителя, а лишь имеет априорное предположение $P(\theta)$, вероятность того, что отправитель принадлежит к данному типу.

В реальности игра носит двусторонний характер, где атакующий и защитник, наблюдая за действиями конкурента, изменяют стратегию своих действий. На рисунке 1 изображен данный процесс.

На этапе 1 защитник выступает в роли отправителя сигнала, а атакующий в роли получателя. Защитник развертывает сеть, настраивает топологию, задает IP-адреса. Злоумышленник различными способами пытается собрать информацию о сети. Такая информация служит основой для проведения сетевой атаки. В нашем случае информация рассматривается как сигнал M_d, выпущенный защитником. Атакующий наблюдает за сигналом M_d, и выбирает наиболее выигрышное ответное действие (оптимальную стратегию атаки).

По ходу игры стороны нападения и защиты постоянно меняются ролями. Каждый этап игры состоит из базовой игры с сигналами, как показано на этапах 2, 3 и i на рисунке 1. На этапе 2 атакующий выбирает стратегию атаки и подает сигнал M_a. Защитник получает сигнал M_a, корректирует априорное суждение о типе атакующего и выбирает соответствующую стратегию защиты. В процессе противостояния сигнал передается в обоих направлениях, и стороны нападения и защиты используют правило Байеса для постепенной корректировки своих оценок истинного типа другой стороны. С точки зрения защитника, условием завершения игры является прекращение атаки со стороны нападающего и прекращение передачи сигналов (этап n на рисунке 1).

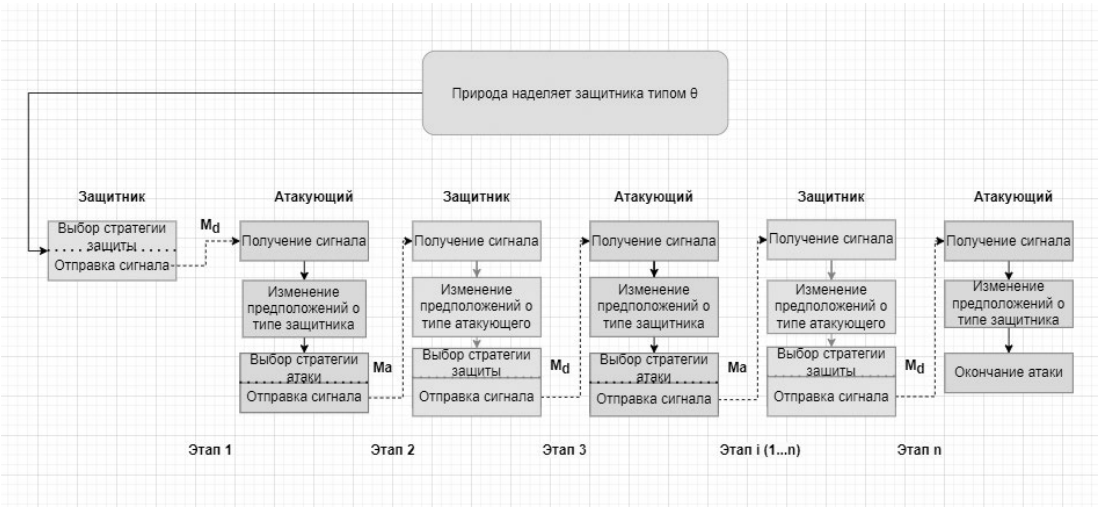

Рис. 1. Многоэтапная двусторонняя сигнальная игра

Построение двусторонней сигнальной модели

Двусторонняя сигнальная модель – это конечная игра, состоящая из нескольких сигнальных игр. В ДСМ атакующий и защитник попеременно выступают в роли отправителя и получателя сигналов.

В двусторонней сигнальной модели (ДСМ) будет использоваться 10 переменных

1) Игроки $N = (N_a, N_d)$, где N_d – защитник, а N_a – атакующий

2) Типы игроков $T = (T_a, T_d)$. тип атакующего $T_a = (\eta_h$ – продвинутый, η_l - обыкновенный); тип защитника $T_d = (\theta_h$ – усиленная система защиты, θ_l – обыкновенная система защиты);

3) $M = (M_a, M_d)$ – сигнал, который подают защитник и атакующий. Сигнал атакующего $M_a = (m_{ah}$ – продвинутый сигнал , m_{al} – обыкновенный сигнал); сигнал защитника M_d = (mdh – усиленный защитный сигнал, m_{dl} – обыкновенный защитный сигнал). Стоит отметить, что в ходе игры отправитель сигнала может попытаться обмануть оппонента, подавая сигналы, которые не соответствуют его собственному типу, с целью ввести соперника в заблуждение, заставив принять неправильный выбор.

4) $S = (D,A)$ – стратегии защитника и атакующего. Стратегия защиты $D = \{d_g | g=1,2,3\ldots.\}$ и стратегия атаки $A = \{a_h | h=1,2,3\ldots.\}$

5) K – стадия игры. $K = (1,2,3\ldots k)$. Сигнальная игра ведется в несколько этапов, и этап игры k представлен в виде ДСМ(k).

6) δ – коэффициент ослабления обмана по ходу игры. После многократных стратегических взаимодействий между атакующим и защищающимся стороны начинают узнавать типы друг друга и сигнал обмана постепенно ослабевает.

7) $P = (P_a, P_d)$ априорная вероятность. P_a - набор убеждений атакующего относительно типа защищающегося. P_d - является набором убеждений защитника относительно типа атакующего.

8) $P = (P_a', P_d')$ апостериорная вероятность. P_a' - является апостериорным набором предположений атакующего о типе защитника. P_d' - является апостериорным набором предположений защитника о типе атакующего.

9) ξ – коэффициент дисконтирования, определяющий величину прибыли на k-этапе.

10) $U = (U_d, U_a)$ обозначает ожидаемый набор выгод для защитника и атакующего.

Определение байесовского равновесия

Для определения стратегии защиты, необходимо найти байесовское равновесие.

В ДСМ(k) равновесие $EQ_k = (m^*(\theta)\ f^*(m),\ P_F'(T|m))$, где - $m^*(\theta)$ стратегия отправителя, $f^*(m)$, - стратегия получателя. $P_F'(T|m)$ – это апостериорная вероятность, которая вычисляется получателем сигнала в соответствии с байесовским правилом на основе априорной вероятности $P(\theta)$, сигнала m и оптимальной стратегии отправителя сигнала $m^*(\theta)$.

Согласно теории игр, равновесие должно удовлетворять условиям (1), (2):

$$f^*(m) \in \underset{f \epsilon F}{arg\,max} \sum P_F'(T|m) U_F(m^*(\theta), f, \theta) \quad (1)$$

$$m^*(\theta) \in \underset{m \epsilon M}{arg\,max}\, U_S(m, f^*(m), \theta) \quad (2)$$

$f^*(m)$ – оптимальная стратегия получателя сигнала после определения апостериорной вероятности $P_F'(\theta|m)$, о типе отправителя сигнала.

$m^*(\theta)$ – оптимальная стратегия отправителя сигнала, после прогнозирования оптимального действия $f^*(m)$ получателя.

Этапы достижения идеального байесовского следующие

Шаг 1. Вычисление оптимальной стратегии $f^*(m)$ на основе сигнала, который получает принимающий.

Шаг 2. Отправитель выбирает оптимальную стратегию $m^*(\theta)$.

Шаг 3. Рассчитать Байесовское равновесие: $EQ_k = (m^*(\theta)\ f^*(m),\ P_F'(T|m))$.

1) На первом этапе игры ДСМ(1) отправителем сигнала является защитник, а получателем атакующий.

Природа выбирает тип защитника. Тип θ_h выбирается с априорной вероятностью p_1, а тип θ_n – с вероятностью $1\text{-}p_1$. Защитник подает сигналы m_{dh} и m_{dl}. Если атакующий получает сигнал защиты m_{dh}, апостериорное заключение атакующего о типе защитника равно $(\alpha_1, 1\text{-}\alpha_1)$, а при получении сигнала m_{dl}, апостериорное заключение атакующего о типе защитника равно $(\beta_1, 1\text{-}\beta_1)$. Затем злоумышленник выбирает стратегию η_h, η_l. Получаем равновесие $EQ1 = (m^*(\theta)\ a^*(m),\ P_a'(\theta))$ для ДСМ(1). На рисунке 2 изображено дерево для этапа ДСМ(1).

2) На втором этапе игры ДСМ(2) отправителем сигнала является атакующий, а получателем защитник. Атакующий выбирает стратегию атаки в соответствии с EQ_1 и посылает сигнал защитнику. В ходе игры ДСМ(1) сторо-

ны нападения и защиты достигли получили определенные данные друг о друге, а значит, сигнал обмана ослабевает. Выбор типа атакующего определяется коэффициентом ослабления сигнала обмана σ и вероятностью $EQ_1(P_F'(T))$ и записывается как $\delta EQ_1(P_F'(T))$. Атакующий выбирает η_h с вероятностью $\delta EQ_1(P_F'(T))$ и η_l с вероятностью $1\text{-}\delta EQ_1(P_F'(T))$. Дерево игры ДСМ(2) показано на рисунке 3.

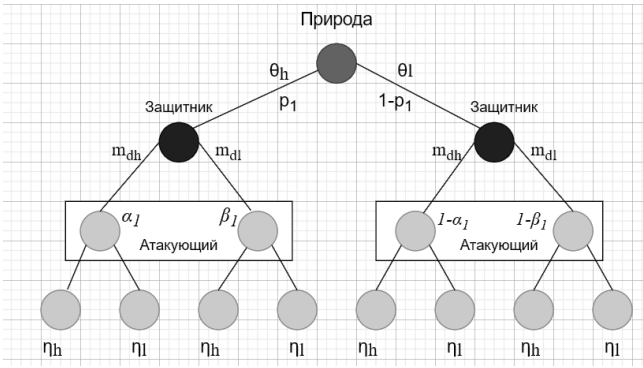

Рис. 2. Дерево для 1 этапа игры

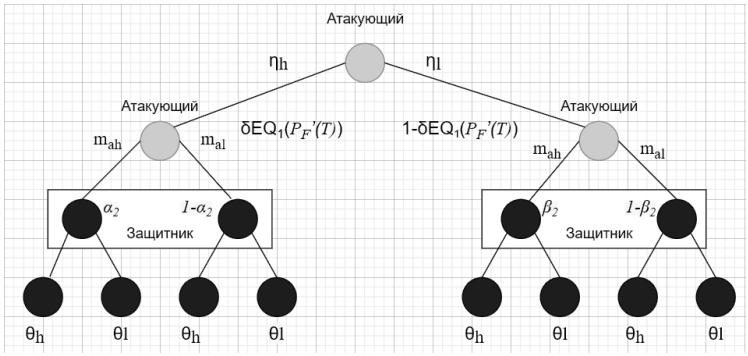

Рис. 3. Дерево для 2 этапа игры

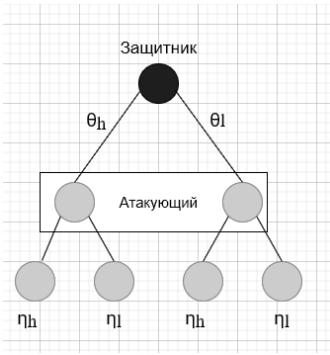

Рис. 4. Дерево для K этапа игры

Игроки на каждом этапе меняются ролями, а значение обманного сигнала уменьшается $\delta_k=\delta^{k-1}$.

На K-ом этапе игры, влияние обманного сигнала полностью исчезнет (например, при δ=0,4 на 7 этапе $\delta_8 = 0{,}4^6 = 0{,}004 \approx 0$: в данном случае K=7)

4) На K-этапе игры ДСМ(K) отправителем сигнала является защитник, а получателем атакующий. Дерево игры показано на рисунке 4.

На данном этапе, обман становится невозможен, поэтому подача ложных сигналов не имеет смысла.

Анализ результатов

Злоумышленник выбирает стратегию атаки, состоящей из нескольких последовательных действий (kill chain). Защитник же выбирает стратегию защиты. В таблице 1 показаны возможные стратегии атакующего и защитника и их расходы на реализацию этих стратегий.

В работе [6] представлены статистические данные для получения значения ущерба системе ($C_{ущ}$) при различных комбинациях стратегий атак и защиты (таблица 2).

Согласно методу расчета затрат [6], прибыль атакующего – это $C_{ущ}$, а затраты – сумма C_a и C_{ao}. Затраты защитника – это сумма $C_{ущ}$, $C_з$ и $C_{зо}$.

Функции прибыли атакующей U_a и обороняющейся U_d сторон могут быть выражены, соответственно, следующим образом (3,4):

$$U_a(a_h, d_g, k) = \sum_{g,h,k} \xi^{k-1} \left[C_{ущ} - C_a - C_{ao} + B_a\right] \quad (3)$$

$$U_d(a_h, d_g, k) = -\sum_{g,h,k} \xi^{k-1} \left[C_{ущ} + C_з + C_{зо} - B_з\right] \quad (4)$$

$B_з$ – выгода защитника при обмане атакующего (при подаче ложного сигнала). Поскольку злоумышленник тратит лишние ресурсы, у защитника появляется время на принятие решений и более эффективное противодействие атаке. $B_з = 100$

B_a – выгода атакующего при обмане защитника. $B_a = 50$

ξ – коэффициент дисконтирования равен 0,5.

δ – коэффициент ослабления сигнала равен 0,6.

Используем вышеописанный метод для получения наступательных и оборонительных выигрышей при различных комбинациях типов стратегий.

Таблица 1.

Стратегии атакующего и защитника

Действия злоумышленника	η_h		η_l		Действия защитника	θ_h		θ_l	
	a_1	a_2	a_3	a_4		d_1	d_2	d_3	d_4
Сканирование сети	+	+	+	+	Honeypot	+	+	+	+
Установка ВПО	+				Honey file	+	+	+	
Переполнение буфера	+	+	+		Антивирусная защита	+	+	+	+
Внедрение кода	+	+			Honey account	+	+		
Повышение привелегий	+	+			Виртуализация сети	+			
Брутфорс			+	+	Honeynet	+	+	+	
DDoS-атака	+		+	+	Разграничение доступа	+	+	+	+
Взлом учетной записи	+		+	+	Многофакторная аутентификация	+			
НСД к ресурсам	+	+			MTD	+	+		
Стоимость атаки (C_a)	**192**	**184**	**96**	**92**	**Стоимость защиты ($C_з$)**	**272**	**256**	**176**	**164**
Стоимость обмана (C_{ao})	**32**	**28**	**12**	**8**	**Стоимость обмана ($C_{зо}$)**	**40**	**32**	**16**	**12**

Таблица 2.

Стоимость ущерба системе

	d_1	d_2	d_3	d_4
a_1	928	952	1056	1072
a_2	908	892	1008	1028
a_3	872	848	912	928
a_4	848	832	884	904

Согласно [5] Природа выбирает тип защитника с вероятностями (0,4, 0,6). Предположим, что защитник с типом θ_h подает сигнал m_{ah}, а злоумышленник выбирает стратегию η_h. В таком случае, мы получаем 4 комбинации стратегий (a_1, d_1), $(a1, d_2)$, (a_2, d_1), (a_2, d_2). Показатели стоимости затрат взяты из таблицы 2, стоимость ущерба берется из таблицы 3.

Найдем функции полезности для атакующего и защитника при выборе комбинации (a_1, d_1) по формулам 5 и 6. Поскольку в данном случае нет обманного сигнала, то выгоды атакующего и защитника равны 0.

$$U_a(a_1 d_1 1) = C_{ущ}(a_1, d_1) - C_a - C_{ao} = 928 - 192 - 0 = 736 \quad (5)$$

В данном случае атакующий не подает сигнала, поэтому $C_{ao} = 0$.

$$U_d(a_1 d_1 1) = -\left[C_{ущ}(a_1, d_1) + C_з + C_{зо}\right] = -[928 + 272 + 0] = -1200 \quad (6)$$

Поскольку защитник не подает ложного сигнала $C_{зо} = 0$.

Так как нам неизвестно, какую стратегию выберет атакующий и защитник, предполагаем, что выбор каждой стратегии равновероятен.

Полученные значения представлены в таблице 3.

Аналогичным образом, используем метод для других комбинаций типов, стратегий

Таблица 3.

Выигрыши защитника и нападающего

	(a_1,d_1)	(a_1,d_2)	(a_2,d_1)	(a_2,d_2)	Ср. знач
U_a	736	724	760	708	732
U_d	-1184	-1114	-1225	-1091	-1184

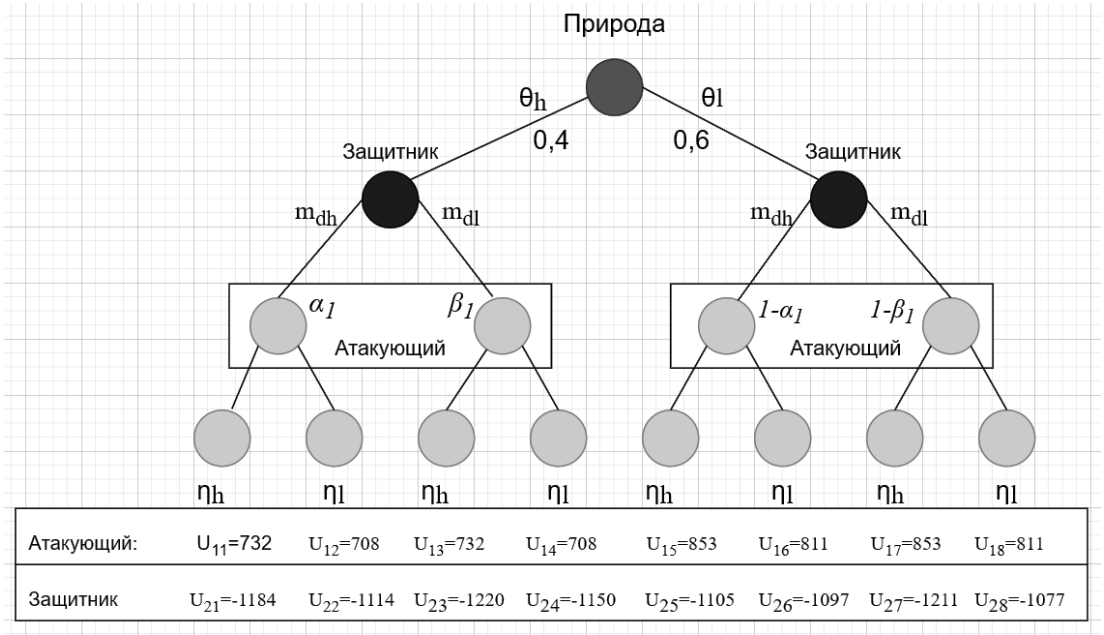

Рис. 5. Игровое дерево для 1 этапа игры ДСМ(1)

и сигналов. Результаты представлены на рисунке 5.

Используя алгоритм решения равновесия, для ДСМ(1) получаем две комбинации типов стратегий:

1) Когда защитник выбирает тип θ_h и подает сигнал m_{dh}, атакующий выбирает стратегию η_h. В этом случае $U_{a1} = -1184$ и $U_{d1} = 732$.

2) Защитник выбирает тип стратегии θ_l и подает сигнал m_{dh}. Па атакующий выбирает тип стратегии η_h. В таком случае $U_{a1} = -1105$ и $U_{d1} = 853$.

Защитник выбирает вариант 2 (θ_l, m_{dh}) в качестве стратегии защиты. Игровое дерево атаки и защиты показано на рисунке 5.

2) Результаты следующих этапов показаны в таблице 4.

Как видно из таблицы, на этапах со второго по шестой защитнику эффективнее использовать обманные сигналы, чтобы заставить злоумышленника выбрать неверную стратегию и уменьшить свои расходы на защиту. Однако с течением времени сигнал ослабевает. В этот момент обман не удастся, поскольку атакующий знает достаточно информации о защитнике. Поэтому, на данном этапе наиболее эффективной является применение усиленной системы защиты.

Предложенная модель двусторонней сигнальной игры имеет существенное значение в области информационной безопасности. С помощью предложенного метода защитник сети может выбрать наиболее эффективную защиту от сетевых атак.

Таблица 4.

Стратегия защиты на различных этапах

Этап	Роль защитника	Выигрыш защитника	Выигрыш атакующего	Стратегия защиты
1	Отправитель	-1105	853	(θ_l, m_{dh})
2	Получатель	-1114,2	821,4	θ_l
3	Отправитель	-1133,4	831,8	(θ_l, m_{dh})
4	Получатель	-1157,8	845	θ_l
5	Отправитель	-1168,2	858,2	(θ_l, m_{dh})
6	Получатель	-1182,6	827,8	θ_l
7	Отправитель	-984	804,4	(θ_h, m_{dh})

Литература

1. Исследование применения технологии deception для предотвращения угроз кибербезопасности. / Путято М. М., Макарян А. С., Чич Ш. М., Маркова В. К. // Прикаспийский журнал: управление и высокие технологии. 2020. №4. Стр. 85-98. URL: https://cyberleninka.ru/article/n/issledovanie-primeneniya-tehnologii-deception-dlya-predotvrascheniya-ugroz-kiberbezopasnosti (дата обращения: 03.04.2024).

2. Афанасьева М.В. Применение данных HONEYPOT-систем для прескриптивной аналитики действий злоумышленника. // Актуальные проблемы современной науки, техники и образования. 2023.№1. С.417

3. Шматова Е. С. Выбор стратегии ложной информационный системы на основе модели теории игр // Вопросы кибербезопасности. 2015. №5 (13). URL: https://cyberleninka.ru/article/n/vybor-strategii-lozhnoy-informatsionnyy-sistemy-na-osnove-modeli-teorii-igr (дата обращения: 13.04.2024).

4. Конюховский П.В. , Шабалин А.А. Теоретико-игровые подходы в анализе стратегий защиты корпоративных информационных систем // International Journal of Open Information Technologies. 2023 №12. URL: https://cyberleninka.ru/article/n/teoretiko-igrovye-podhody-v-analize-strategiy-zaschity-korporativnyh-informatsionnyh-sistem (дата обращения: 12.04.2024).

5. J. Pawlick and Q. Zhu, "Deception by design: evidence-based signaling games for network defense," 2015. URL: https://archive.org/details/arxiv-1503.05458/page/n23/mode/2up (дата обращения: 02.04.2024).

6. Y. Hu, H. Zhang, Y. Guo, T. Li, and J Ma, "A novel attack-and-defense signaling game for optimal deceptive defense strategy choice," Wireless Communications and Mobile Computing, vol. 2020. URL: https://www.hindawi.com/journals/wcmc/2020/8850356/ (date of application: 10.04.2024).

7. Голдуева Д.А., Мокшанина М. А. Принятие решений в условиях неопределенности на основе теории игр с природой. // Вестник ПензГУ. 2020. №4 (32). URL: https://cyberleninka.ru/article/n/prinyatie-resheniy-v-uslovii-neopredelennosti-na-osnove-teorii-igr-s-prirodoy (дата обращения: 14.04.2024).

References

1. Issledovaniye primeneniya tekhnologii deception dlya predotvrashcheniya ugroz kiberbezopasnosti. / Putyato M. M., Makaryan A. S., Chich SH. M., Markova V. K. // Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii. 2020. №4. Str. 85-98. URL: https://cyberleninka.ru/article/n/issledovanie-primeneniya-tehnologii-deception-dlya-predotvrascheniya-ugroz-kiberbezopasnosti (data obrashcheniya: 03.04.2024).

2. Afanas'yeva M.V. Primeneniye dannykh HONEYPOT-sistem dlya preskriptivnoy analitiki deystviy zloumyshlennika. // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. 2023.№1. S.417

3. Shmatova Ye. S. Vybor strategii lozhnoy informatsionnyy sistemy na osnove modeli teorii igr // Voprosy kiberbezopasnosti. 2015. №5 (13). URL: https://cyberleninka.ru/article/n/vybor-strategii-lozhnoy-informatsionnyy-sistemy-na-osnove-modeli-teorii-igr (data obrashcheniya: 13.04.2024).

4. Konyukhovskiy P.V., Shabalin A.A. Teoretiko-igrovyye podkhody v analize strategiy zashchity korporativnykh informatsionnykh sistem // International Journal of Open Information Technologies. 2023 №12. URL: https://cyberleninka.ru/article/n/teoretiko-igrovye-podhody-v-analize-strategiy-zaschity-korporativnyh-informatsionnyh-sistem (data obrashcheniya: 12.04.2024).

5. Konyukhovskiy P.V., Shabalin A.A Game-theoretic Approaches in The Analysis of Corporate Information Systems Protection Strategies // International Journal of Open Information Technologies. 2023 №12. URL: https://cyberleninka.ru/article/n/teoretiko-igrovye-podhody-v-analize-strategiy-zaschity-korporativnyh-informatsionnyh-sistem (date of application: 12.04.2024).

6. J. Pawlick and Q. Zhu, "Deception by design: evidence-based signaling games for network defense," 2015. URL: https://archive.org/details/arxiv-1503.05458/page/n23/mode/2up (date of application: 02.04.2024).

7. Golduyeva D.A., Mokshanina M. A. Prinyatiye resheniy v usloviyakh neopredelennosti na osnove teorii igr s prirodoy. // Vestnik PenzGU. 2020. №4 (32). URL: https://cyberleninka.ru/article/n/prinyatie-resheniy-v-uslovii-neopredelennosti-na-osnove-teorii-igr-s-prirodoy (data obrashcheniya: 14.04.2024).

КОТЕЛЬНИКОВ Никита Дмитриевич, студент 5 курса по специальности «Информационная безопасность автоматизированных систем», ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина 38. E-mail: nick-kotelnik@yandex.ru

АФАНАСЬЕВА Маргарита Владимировна, ассистент кафедры «Информатики и информационной безопасности», ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина 38. E-mail: nansy_stokli@mail.ru

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующий кафедрой «Информатики и информационной безопасности», ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

KOTELNIKOV Nikita Dmitrievitch, 5th year student majoring in "Information Security of Automated Systems", Federal State Budgetary Educational Institution of Higher Education, Magnitogorsk State Technical University named after G.I. Nosov. 455000, Magnitogorsk, Lenin Ave. 38. E-mail: nick-kotelnik@yandex.ru

AFANASYEVA Margarita Vladimirovna, Assistant of the Department of Computer Science and Information Security, Federal State Budgetary Educational Institution of Higher Education, Magnitogorsk State Technical University named after G.I. Nosov. 455000, Magnitogorsk, Lenin Ave. 38. E-mail: nansy_stokli@mail.ru

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Head of the Department of Computer Science and Information Security, Federal State Budgetary Educational Institution of Higher Education, Magnitogorsk State Technical University named after G.I. Nosov. 455000, Magnitogorsk, Lenin Ave. 38. E-mail: inna_barankova@mail.ru