Управление рисками и безопасностью

Моделирование развития олигополистических рынков при наличии киберугроз

Л.Е. Варшавский[I,II]

[I] Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Россия
[II] Федеральное государственное бюджетное учреждение Центральный экономико-математический институт Российской академии наук" г. Москва, Россия.

Аннотация. В статье рассматривается динамическая игровая модель развития олигополистических рынков в условиях кибератак на производственную инфраструктуру. Компании-участники рынка используют оптимальные по Нэшу, с позиций чистой текущей стоимости (NPV), стратегии ввода мощностей с учетом того, что целью кибератак является минимизация этого показателя. Рассматриваются результаты расчетов показателей условного олигополистического рынка при разных гипотезах о восприятии олигополистами интенсивности киберугроз.
Ключевые слова: *кибератаки, динамические игры, олигополистические рынки.*
DOI: 10.14357/20790279200203

Введение

В связи с форсированным внедрением информационно-коммуникационных технологий (ИКТ), осуществляемым без должного анализа связанных с ними рисков и угроз, повышается роль исследований в области кибербезопасности, и, в частности, экономических аспектов, связанных с обеспечением приемлемых уровней обеспечения безопасности критической инфраструктуры, производства, а также товарных рынков, особенно рынков высокотехнологичной продукции. Актуальность подобных исследований обусловлена и тем фактом, что в настоящее время прямые и косвенные затраты в мире, связанные с киберпреступлениями, приближаются к 1 трлн. долл., а их доля в мировом ВВП – к 1 %[1]. По некоторым оценкам потери только российской экономики от кибератак в 2019 году могли составить 1,6–1,8 трлн руб.[2].

Ещё в 2015 г. средние затраты американских компаний численностью занятых свыше 1000 чел. составляли 15 млн. долл[3]. Прямые потери от одной успешной кибератаки оценивались в 5 млн. долл.[4] В 2019 г. в американских компаниях с годовыми уровнями дохода свыше 1 млрд. долл. средние затраты на восстановление после одной успешной кибератаки составляли 4.6 млн. долл.[5]. В связи с

[1] URL: https://www.cnbc.com › 2018/02/22 › cybercrime-pandemic-may-have-cost-$600 billion (Доступ 15.11.2019).

[2] URL: http://www.ng.ru/economics/2019-11-05/1_7718_hakers.html (Доступ 10.11.2019).

[3] URL: http://www.csoonline.com/article/2989302/cyber-attacks-espionage/average-business-spends-15-million-battling-cybercrime.html (Доступ 15.10.2019).

[4] URL: https://www.appknox.com/blog/cybersecurity-statistics-2019 (Доступ 17.11.2019).

5 URL: https://techbeacon.com/security/31-cybersecurity-stats-matter (Доступ 15.11.2019).

возрастающими киберугрозами бизнес непрерывно увеличивает затраты на кибербезопасность. Особенно высокие затраты по этой статье характерны для компаний банковско-финансового сектора и сектора информационных технологий. Так, финансовый гигант.P. Morgan Chase & Co. в 2017 г. расходовал на кибербезопасность 600 млн. долл. (в 2016 г. – 500 млн. долл.). Microsoft Corp. планировал затрачивать на кибербезопасность не менее 1 млрд. долл. ежегодно[6]. В итоге, во всем мире происходит неуклонный рост затрат на кибербезопасность, которые в 2019 г. по оценкам компании Gartner достигли 124 млрд. долл., что составляет 4% от затрат на информационно-коммуникационные технологии (ИКТ), и что превышает уровень 2004 г. в 35 раз![7]

Особую тревогу вызывают участившиеся киберпреступления, направленные против критически важной инфраструктуры. Так, в последние годы отмечается рост кибератак на энергосистемы и объекты жизнеобеспечения городов и стран. По данным Group-IB в 2019 г. российские организации подвергались примерно 50000 кибератакам[8]. Успешному проведению кибератак способствует то, что многие промышленные объекты оснащены старыми АСУ ТП, при разработке которых не учитывалась возможность масштабных киберпреступлений. В перспективе, по мере расширения масштабов распространения облачныъ вычислений и Интернета вещей следует ожидать усиления интенсивности кибератак. В этом отношении отмечается, что даже широкомасштабное использование «умных» счетчиков, устанавливаемых повсеместно быстрыми темпами, может привести к нарушениям в работе крупных энергосистем на период до нескольких месяцев[9]. Риски, связанные с целенаправленным выведением техники и оборудования из эксплуатации, возрастают и по мере увеличения сложности энергетических объектов и сетей[10]. На возрастающие риски повреждения своих производственных мощностей в результате кибератак всё более активно указывают крупнейшие высокотехнологичные компании, такие, как, например, Intel, General Electric и др.

В связи с вышеизложенным, в настоящее время происходит активизация исследований в области повышения надежности киберфизических систем и их устойчивости к кибератакам. В то же время, недостаточной внимание уделяется исследованию экономических проблем, связанных с функционированием экономических систем и рынков в условиях киберугроз, особенно динамическим аспектам развития рынков, подвергающихся кибератакам. Среди небольшого числа теоретических работ, посвященных этой теме следует отметить статьи [1], [2] и связанные с ними работы, а также [3]. В первых двух статьях исследуется целесообразный уровень затрат на кибербезопасность в статике. Последняя из перечисленных работ посвящена вопросам оптимизации инвестиций в кибербезопасность (у защищающейся стороны) и в проведение кибератаки (у атакующей стороны) на основе дифференциальной игровой модели.

Необходимо отметить, что ввиду отсутствия надежных статистических данных о числе кибератак и вызванных ими потерь, возникают естественные трудности при исследовании реальных экономических процессов. Поэтому предлагаемые исследователями методические подходы и модели приходится иллюстрировать на примере условных экономических объектов и рынков.

В настоящей статье рассматривается игровой подход к исследованию динамики показателей олигополистических рынков, участники которых подвергаются кибератакам на производственную инфраструктуру. Анализируются результаты расчетов показателей условного рынка в соответствии с 3 сценариями.

1. Модель динамики показателей олигополистических рынков в условиях кибератак

Проводимый в настоящей статье анализ основан на использовании агрегированной динамической модели рационального поведения участников олигополии в виде линейной динамической игры по Нэшу - Курно с квадратичным критерием, в которой участвуют N фирм-олигополистов. Предполагается, что целью кибератак является уничтожение производственных мощностей участников рынка.

Центральным блоком модели является следующая зависимость, связывающая объемы товарного производства Q_{it} со входной переменной u_{it} (вводом мощностей), i – индекс фирмы, $i = 1,2,...,N$, t – индекс года:

$$Q_{it} = W_i(z)\,u_{it} + Q_{0it} - W_{0i}(z)\,\chi_i v_{it}, \qquad (1)$$

где $W_i(z) = B_i(z)/A_i(z)$ – передаточная функция, причем $A_i(z)$, $B_i(z)$ – полиномы относительно

[6] URL: https://cybersecurityventures.com/cybersecurity-market-report/ (Доступ 25.11.2019).

[7] URL: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 (Доступ 13.09.2019).

[8] URL: https://www.vedomosti.ru/technology/articles/2019/04/17/799417-kolichestvo-kiberatak(Доступ 15.11.2019) (Доступ 10.09.2019).

[9] URL: https://phys.org/news/2017-08-smart-electrical-grids-vulnerable-cyber.html (Доступ 15.11.2019).

[10] URL: http://www.finmarket.ru/news/493477 (Доступ 25.11.2019).

переменной z, представляющей собой оператор сдвига: $zx_t = x_{t+1}, Q_{0it}$ – слагаемое, характеризующее начальные условия, $\chi_i = p(\mu_i) * g_i$ – средняя величина падения производства из-за уничтожения производственной мощности в результате одной кибератаки, $p(\mu_i)$ – вероятность успешного отражения кибератаки, зависящая от μ_i – соотношения между дополнительными затратами на кибербезопасность и средними производственными издержками (OPEX), g_i – потери мощности и продукции в результате одной кибератаки; v_{it} – число кибератак, $W_{0i}(z)$ – передаточная функция, связывающая число кибератак с падением мощности и производства продукции. Другой блок модели – обратная функция спроса. В модели предполагается баланс суммарного спроса D_t и предложения Q_t, т.е. $D_t = Q_t = \sum_{i=1}^{N} Q_{it}$ и линейная зависимость цены на рынке P_t от объема спроса:

$$P_t = a - bD_t = a - bQ_t, \qquad (2)$$

где Q_{Ft} – суммарный объем производства малых компаний-ценополучателей, a, b – параметры.

Предполагается, что олигополисты используют скользящее планирование и в каждый момент времени τ максимизируют чистую текущую стоимость (NPV) с учетом того, что участники кибератак стремятся нанести компаниям максимальный ущерб:

$$J_{\tau i} = \sum_{t=\tau}^{\tau+Tp} \beta^t [(P_t - PL_i)Q_{it} - \frac{1}{2}\rho_{1i}u_{it}^2 + \frac{1}{2}\rho_{2i}v_{it}^2] \to \max_{u_{it}} \min_{v_{it}} \qquad (3)$$

где: $\beta = 1/(1+r)$ – дисконтирующий множитель, соответствующий ставке дисконтирования r; P_t – цена продукции; c_i – средние производственные издержки (без амортизации); $PL_i = (1+\mu_i)c_i + q_i/W(1+r_i)$ – приведенные затраты i-ой фирмы, q_i – стоимость единицы мощностей; $\frac{1}{2}\rho_{1i}u_{it}^2$, $\frac{1}{2}\rho_{2i}v_{it}^2$ – затраты регулирования, характеризующие соответственно инвестиционные возможности олигополистов (см., например, [4], [5]) и их восприятие интенсивности кибератак, с коэффициентами, $\rho_{1i} > 0$, $\rho_{2i} > 0$, $i = 1,2,...,N$ –; T_p – период скользящего планирования (для упрощения записи формул ставки налогов приняты равными нулю). Управляющими переменными для олигополистов в модели являются объемы ввода мощностей u_{it}, а также доли затрат на кибербезопасность μ_i $i = 1,2,...,N$.

В данной статье при проведении расчетов использован подход к расчету оптимальных по Нэшу-Курно разомкнутых (open-loop), стратегий, основанный на представлении модели (1)-(3) в пространстве состояний и использовании обобщенных (generalized) матричных уравнений Риккати (см., например, [6], [7]). При этом модель (1)-(4) предварительно представлена в эквивалентной форме в пространстве состояний:

$$X_t = AX_{t-1} + \sum_{i=1}^{N}(B_i u_{it} + D_i v_{it}), \qquad (4)$$

$$J_{\tau i} = \sum_{t=\tau}^{\tau+Tp} \beta^t (\frac{1}{2}X_t' H_i X_t - C_{0i}' X_t - \frac{1}{2}\rho_{1i}u_{it}^2 + \frac{1}{2}\rho_{2i}v_{it}^2) \to \max_{u_{it}} \min_{v_{it}}, \qquad (5)$$

где матрицы и векторы A, B_i, D_i, H_i, C_{0i}, X_t, $i = 1,2...N$ связаны с параметрами и переменными исходной модели. Получаемые оптимальные стратегии участников олигополии uit линейно связаны с вектором состояния системы (5) соотношением:

$$u_{it} = K_{it}X_{t-1} + \eta_{it} \qquad (6)$$

в котором K_{it} и η_{it} – векторы, зависящие от решений обобщенных уравнений Риккати [6].

Основная трудность при практическом использовании в прогнозных исследованиях предлагаемого подхода состоит в адекватной оценке коэффициентов ρ_{1i} и ρ_{2i}. Для этого целесообразно обратиться к соотношениям оптимальности, получаемым с помощью частотного метода (операционного исчисления). Так, используя подход к решению данной задачи, основанный на применении операционного исчисления (см. [5],[8]), можно показать, что в случае, когда $T_p \to \infty$ [11], при равновесии по Нэшу-Курно для задачи (1)-(3) справедливы следующие соотношения (для упрощения формул, далее принято, что $Q_{0it} \equiv 0$, $i = 1,2...N.$):

$$v_{it} = \frac{\rho_{1i}}{\rho_{2i}}\chi_i \left[\frac{W_{0i}((\beta z)^{-1})}{W_i((\beta z)^{-1})}\right] u_{it} \qquad (7)$$

$$Q_{it} = \frac{\Gamma_i(z,(\beta z)^{-1})}{b}(p_t - PL_i), \qquad (8)$$

где:

$$\Gamma_i[z,(\beta z)^{-1}] = \frac{b\left[W_i(z)W_i((\beta z)^{-1}) - \frac{\rho_{1i}}{\rho_{2i}}\chi_i^2 W_{0i}(z)W_{0i}((\beta z)^{-1})\right]}{\rho_{1i} + \left[W_i(z)W_i((\beta z)^{-1}) - \frac{\rho_{1i}}{\rho_{2i}}\chi_i^2 W_{0i}(z)W_{0i}((\beta z)^{-1})\right]}, \quad i = 1,2...N \qquad (9)$$

$$P_t = \frac{1}{1 + \sum_{i=1}^{N}\Gamma_i[z,(\beta z)^{-1}]}\{a + \sum_{i=1}^{N}\Gamma_i[z,(\beta z)^{-1}]PL_i\}. \qquad (10)$$

[11] Следует отметить, что целесообразность использования операционного исчисления обусловлена тем, что во многих случаях значения расчетных показателей при бесконечном (TP →∞) и при конечном периоде скользящего планирования (TP≈20÷30) близки.

$\frac{\rho_{1i}}{\rho_{2i}}\chi_i$, тем сильнее предполагаемое i-ой компанией количество кибератак v_{it} связано со входной переменной u_{it} и соответственно, с производственными инвестициями ($Inv_{it} = q_i u_{it}$). При постоянных значениях коэффициентов модели (1)-(3), в силу свойств Z–преобразования (см. [9]), имеет место следующая зависимость между числом кибератак и объёмом вводимых мощностей в установившемся состоянии:

$$v_{i\infty} = \lim_{z\to 1} {}_{it}\ \frac{\rho_{1i}}{\rho_{2i}}\chi_i\left[\frac{W_{0i}((\beta z)^{-1})}{W_i((\beta z)^{-1})}\right]u_{i\infty} =$$

$$= \frac{\rho_{1i}}{\rho_{2i}}\chi_i\left[\frac{W_{0i}(1+r)}{W_i(1+r)}\right]u_{i\infty} = CAAI_i * \left[\frac{W_{0i}(1+r)}{W_i(1+r)}\right]u_{i\infty}, \quad (11)$$

где $\mathrm{CAAI_i} = \frac{\rho_{1i}}{\rho_{2i}}\chi_i$. В дальнейшем этот показатель будет именоваться индексом восприятия интенсивности кибератак. Очевидно для поддержания $\mathrm{CAAI_i}$ на постоянном уровне при изменении вероятности отражения атак за счет увеличения затрат на кибербезопасность, а также при постоянном коэффициенте ρ_{1i}, принимаемый i-м олигополистом коэффициент ρ_{2i} должен уменьшаться. В других случаях, в зависимости от предполагаемого характера изменения $\mathrm{CAAI_i}$, этот коэффициент может как уменьшаться, так и увеличиваться. Таким образом, предположения олигополистов об изменении индексов $\mathrm{CAAI_i}$ могут быть положены в основу формирования сценариев развития рынков.

Формулы (7)-(9), (2) могут быть использованы для определения соотношений между коэффициентами ρ_{1i} и ρ_{2i}, соответствующих желаемым оптимальным долговременным уровням товарной продукции $Q_{i\infty}$, i=1, 2…N, т.е. при $t \to \infty$. Так, в ввиду (2), (8), (9) справедливо:

$$P_\infty = a - bQ_\infty, \quad (2a)$$

$$\frac{bQ_{i\infty}}{(p_\infty - PL_i)} = \Gamma_i(z,(\beta z)^{-1})\Big|_{z=1} = \frac{b\left[W_i(1)W_i(1+r) - \frac{\rho_{1i}}{\rho_{2i}}\chi_i^2 W_{0i}(1)W_{0i}(1+r)\right]}{\rho_{1i} + b\left[W_i(1)W_i(1+r) - \frac{\rho_{1i}}{\rho_{2i}}\chi_i^2 W_{0i}(1)W_{0i}(1+r)\right]}, \quad (9a)$$

(при выводе (9а), как и (11), использовалось свойство Z–преобразования см. [9]). Из последнего соотношения можно при известных ρ_{1i} определить соотношение $\frac{\rho_{1i}}{\rho_{2i}}$:

$$\frac{\rho_{1i}}{\rho_{2i}} = \frac{W_i(1)W_i(1+r) - \rho_{1i}\ \Gamma_i(1,1+r)/[b(1-\Gamma_i(1,1+r)]}{\left[\chi_i^2 W_{0i}(1)W_{0i}(1+r)\right]},$$

$$i = 1,2...N \quad (12)$$

и ρ_{2i}:

$$\rho_{2i} = \frac{\rho_{1i}\chi_i^2 W_{0i}(1)W_{0i}(1+r)}{W_i(1)W_i(1+r) - \rho_{1i}\ \Gamma_i(1,1+r)/[b(1-\Gamma_i(1,1+r)]} \quad (13)$$

Наконец, следует отметить, что соотношение (7) остается справедливым и при изменяющихся во времени значениях коэффициентов ρ_{1it} и ρ_{2it}, а также g_{it}. В этом случае при разработке прогнозных сценариев могут быть использованы гипотезы об изменении интенсивности и эффективности кибератак а, следовательно, и индекса $\mathrm{CAAI_i}$ во времени.

2. Подходы к прогнозированию показателей олигополистического рынка (условный пример)

На условном примере триополии ниже рассматриваются изложенные выше подходы к прогнозированию, основанные на следующих гипотезах: 1. о постоянстве восприятия интенсивности киберугроз олигополистами (постоянстве индексов $\mathrm{CAAI_i}$); 2. о переменности коэффициентов $\rho_{2i}\ u\ g_i; i = 1,2,3$ и, следовательно $\mathrm{CAAI_i}$; 3. о стремлении олигополистов обеспечить себе желаемые доли на рынке.

В качестве центрального блока модели рассматривается, модель освоения мощностей [10], для которой соотношения типа (1) для каждого олигополиста в пространстве состояний могут быть представлены в виде:

$$X_{it} = A_i X_{it-1} + B_i u_{it} + D_i v_{it}, \quad (14)$$

где $X_{it} = (x_{i1t}, x_{i2t}, x_{i3t})'$ – вектор-столбец,

$$A_i = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0.95 \end{pmatrix};\quad \mathrm{B_i} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix};\quad \mathrm{D_i} = \begin{pmatrix} 0 \\ 0 \\ -\chi_i \end{pmatrix} \quad (15)$$

$$Q_{it} = (k_o, k_1, 1)X_{it},\ 0 < k_o < k_1 < 1,\quad i = 1,2...N.$$

В базовом варианте для всех сценариев значения удельных производственных затрат на единицу производимой продукции (OPEX) составляют $c_1 = c_2 = 100,\ c_3 = 85$; удельных капитальных вложений на единицу вводимой мощности $q_1 = q_2 = q_3 = 100$, доли затрат на кибербезопасность от величины OPEX $\mu_1 = \mu_2 = \mu_3 = 0.05$, а процентной ставки – $r = 0.03$. Приняты следующие значения коэффициентов освоения мощностей: $k_o = 0.4;\ k_1 = 0.7$. Значения коэффициентов ρ_{1i}, ρ_{2i} представлены в таблице 1.

Табл. 1

Значения коэффициентов ρ_{1i} , ρ_{2i} в базовом варианте

i=	ρ_{1i}	ρ_{2i}
1	70	4.3
2	70	4.3
3	50	3

Таким образом, третья компания, имеющая лучшие экономические показателя (c_3, ρ_{13}), является компанией-лидером. Принято также, что вероятность успешного отражения кибератак связана с долей затрат на кибербезопасность от величины OPEX μ_i зависимостью $p_i = \exp(-40\mu_1),\ i = 1,2,3$, а также, для упрощения, что во всех расчетных вариантах компании руководствуются одинаковой долей затрат на кибербезопасность $\mu_1 = \mu_2 = \mu_3$. Параметры функции спроса (2) имеют следующие значения: $a = 160:\ b = 0{,}15$.

3.1. Прогнозирование на основе гипотезы 1.

Данная гипотеза состоит в том, что олигополисты при разработке стратегий развития исходят из предположения об относительно стабильной интенсивности атак (при этом индекс $\mathrm{CAAI_i} = \frac{\rho_{1i}}{\rho_{2i}}\chi_i$ остается постоянным даже при уменьшении вероятности успешных атак $p(\mu_i)$ и соответственно росте затрат на кибербезопасность μ_i).

Расчеты при следующих значениях индексов восприятия интенсивности атак: $\mathrm{CAAI_i} = 2.204, i = 1,2; \mathrm{CAAI_3} = 2.256$ показы-

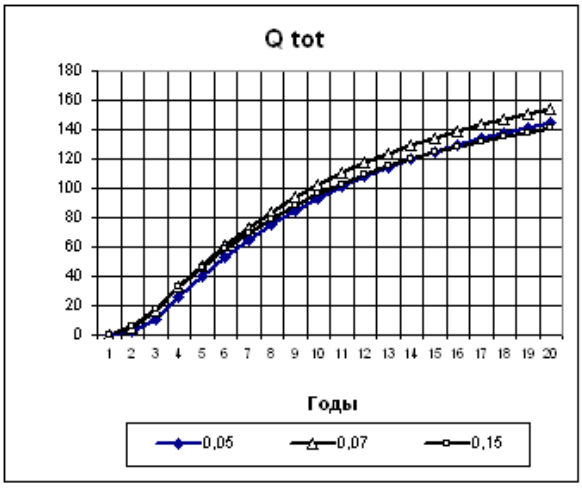

Рис. 1. Динамика суммарных объемов товарной продукции (Q_{tot}, тыс. усл. ед.) в триополии при разных долях затрат на кибербезопасность (μ=0,05; 0,07; 0,15) при справедливости гипотезы 1.

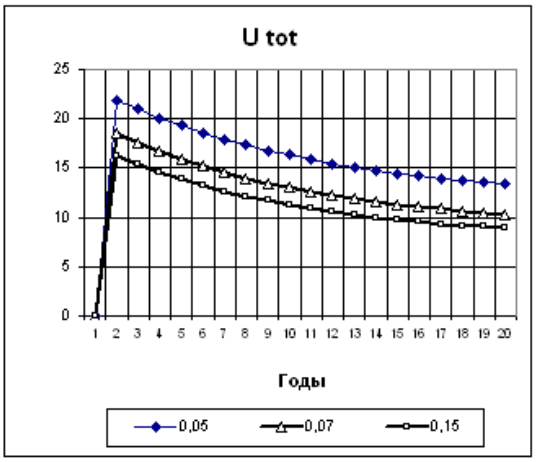

Рис. 2. Динамика суммарных объемов ввода мощностей (U_{tot}, тыс. усл. ед.) в триополии при разных долях затрат на кибербезопасность (μ=0,05; 0,07; 0,15) при справедливости гипотезы 1.

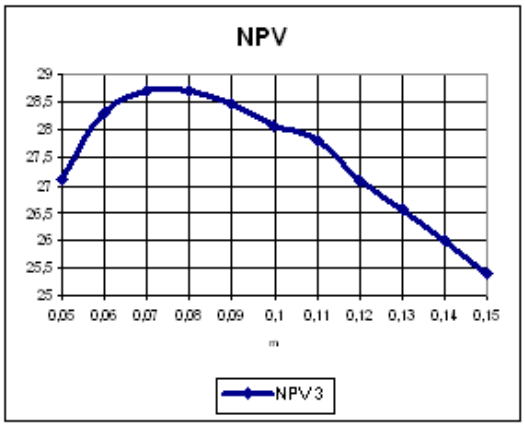

Рис. 3. Зависимость показателя NPV за 20 лет (млн. усл. ед.) третьей компании в триополии от доли затрат μ на кибербезопасность при справедливости гипотезы 1.

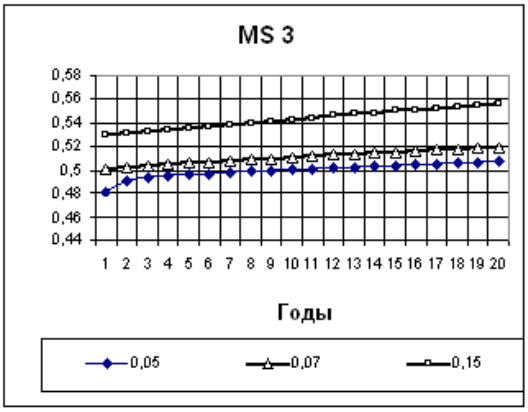

Рис. 4. Динамика рыночной доли третьей компании (MS 3) в триополии при разных долях затрат на кибербезопасность μ (μ=0,05; 0,07; 0,15) при справедливости гипотезы 1.

вают, что увеличение до определенного предела затрат компаний на кибербезопасность (в долях от операционных затрат) приводит к росту ряда ключевых экономических показателей, что, в частности, отражается на увеличении показателей чистой текущей стоимости (NPV) в компании-лидере. Дальнейший рост этих затрат приводит к снижению объёмов производства, а также показателей эффективности этого участника рынка. Вместе с тем, рыночная доля компаний-лидеров, имеющих меньшие удельные затраты на производство (OPEX), может возрастать и с дальнейшим ростом доли выделяемых затрат на кибербезопасность. Динамика показателей триополии при справедливости первой гипотезы представлена на рис. 1-4.

3.2. Прогнозирование на основе гипотезы 2.

В этом случае участники рынка руководствуются гипотезой о переменных во времени значениях коэффициентов ρ_{2it} u $g_{it}; i = 1,2,3.$ Расчеты в данной работе проведены при разных темпах прироста этих коэффициентов для базового сценария (таблица 2). Они показывают, что существенное превышение темпов роста коэффициента восприятия интенсивности кибератак $\delta\rho_{2it}$ над темпами роста коэффициента потерь δg_{it}, т.е. при $\delta\rho_{2it} > \delta g_{it}; i = 1,2,3$ приводит к заметному увеличению объемов производства товарной продукции за счет значительного уменьшения предполагаемой интенсивности атак и, соответственно, потерь (рис. 5, 6).

Табл. 2

Значения темпов роста коэффициентов g_i, ρ_{2i}

Вариант	$\delta g_1 = \delta g_2 = \delta g_3$	$\delta\rho_{21} = \delta\rho_{22} = \delta\rho_{23}$
1	1.00	1.00
2	1.0100	1.0100
3	1.0100	1.1110

3.3. Прогнозирование на основе гипотезы 3.

В этом случае предполагается, что олигополисты стремятся обеспечить следующие объёмы выпуска товарной продукции в долгосрочной перспективе: $Q_{1\infty} = Q_{2\infty} = 45$ и $Q_{3\infty} = 95$ тыс. единиц. Ниже проведены результаты расчетов для двух вариантов с равными объемами желаемой товарной продукции, но различающихся значениями отношений между коэффициентами

$\frac{\rho_{1i}}{\rho_{2i}}$, i=1,2,3 (таблица 3), при тех же значениях

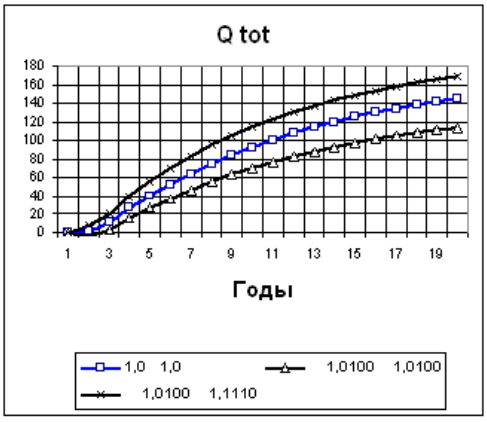

Рис. 5. Динамика суммарных объемов товарной продукции (Q_{tot}, тыс. усл. ед.) в триополии при разных темпах роста величины ущерба от одной атаки δg_i и коэффициентов $\delta\rho_{2i}$ i=1,2,3.

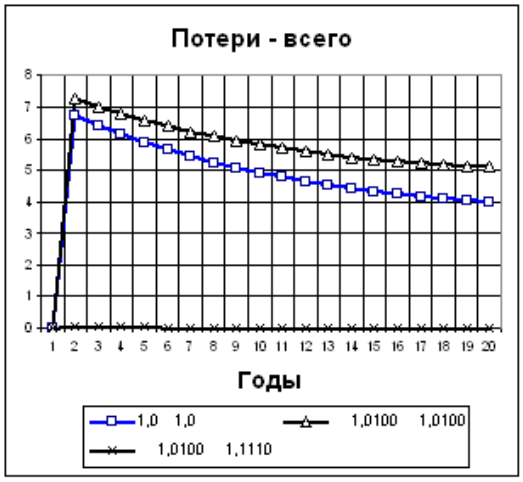

Рис. 6. Динамика суммарных объемов средних потерь мощности в триополии результате кибератак (тыс. усл. ед.) при разных темпах роста величины ущерба от одной атаки δg_i и коэффициентов $\delta\rho_{2i}$ i=1,2,3.

остальных параметров модели (1)-(3), что и в базовом варианте.

Вариант 2, характеризующийся существенно большими значениями этих отношений, соответствует значительному росту интенсивности кибератак и, как следствие этого, инвестиций, что связано с необходимостью компенсации большего ущерба из-за дополнительных потерь,

Табл. 3

Значения коэффициентов ρ_{1i}, ρ_{2i} в вариантах 1 и 2

Вариант	$Q_{1\infty} = Q_{2\infty} = 45$	$\rho_{21} = \rho_{22}$	ρ_{13}	ρ_{23}
1	75.00	19.76	55.00	8,05
2	50.00	2.25	30,00	0,98

вызываемых большим числом атак. Среднее значение NPV в триополии во втором варианте ниже, чем в первом (рис. 7-9, таблица 4).

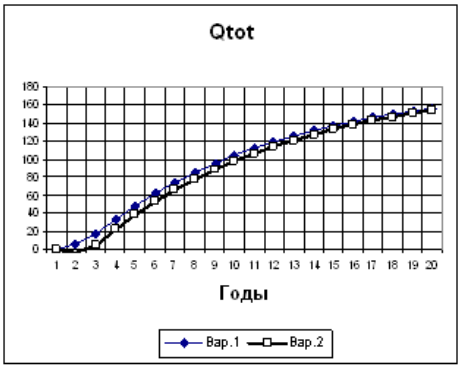

Рис. 7. Динамика суммарных объемов товарной продукции (Q_{tot}, тыс. усл. ед.) в триополии при разных значениях коэффициентов ρ_{1i}, ρ_{2i}.

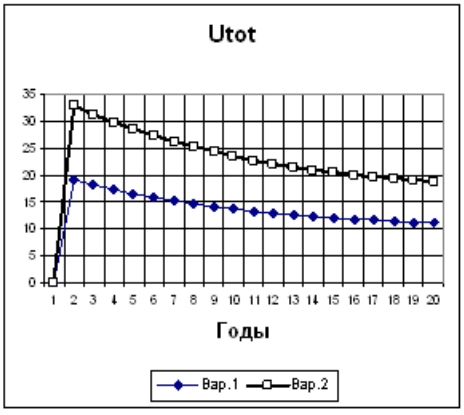

Рис. 8. Динамика суммарных объемов ввода мощностей (U_{tot}, тыс. усл. ед.) в триополии при разных значениях коэффициентов ρ_{1i}, ρ_{2i}.

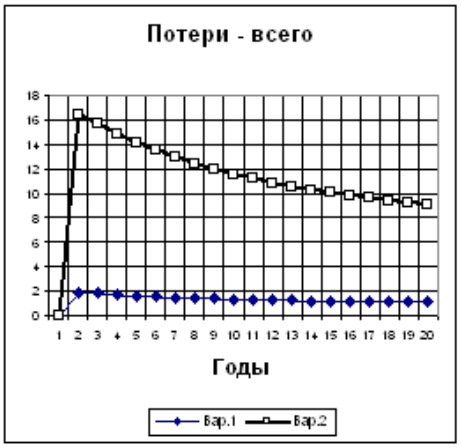

Рис. 9. Динамика суммарных объемов средних потерь товарной продукции (тыс. усл. ед.) в триополии при разных значениях коэффициентов ρ_{1i}, ρ_{2i}.

Табл. 4

Расчетные значения показателей NPV компаний, млн. усл. ед.

Вариант	NPV 1,2	NPV 3
1	9,843	28,582
2	9,493	25,773

Вместе с тем, дополнительные расчеты показывают, что при отсутствии кибератак объемы производства, соответствующие наиболее оптимистическому первому варианту, могли бы быть достигнуты при меньших объёмах инвестиций и эксплуатационных затрат OPEX (соответственно на 11% и на 5%), причем показатель NPV был бы при этом выше для каждой из двух первых компаний на 12% , а для третьей (компании-лидера) — на 9%.

Заключение

Форсированная цифровизация без должного учета рисков, связанных с киберугрозами, и без обеспечения высокого уровня кибербезопасности приводит к серьезным экономическим потерям.

Рассмотренный игровой подход позволяет получить предварительную оценку целесообразных затрат на кибербезопасность для участников олигополистических рынков, а также разрабатывать сценарии поведения участников рынка с учетом нестационарной во времени интенсивности кибератак.

Использование введенного в статье индекса восприятия фирмами интенсивности кибератак упрощает формирование гипотез, закладываемых в основу сценариев развития рынков.

Литература

1. *Gordon L. A. and M. P. Loeb*. The Economics of Information Security Investment//*ACM Transactions on Information and System Security*, 2002. – pp. 438-457.
2. *Gordon L A., Loeb M. P., Zhou Lei.* Investing in Cybersecurity: Insights from the Gordon-Loeb Model// Journal of Information Security, 2016. – No7. – pp. 49-59.
3. URL: http://ceur-ws.org/Vol-2040/paper14.pdf (Доступ 20.11.2020).
4. *Варшавский Л.Е.* Исследование инвестиционных стратегий фирм на рынках капитало- и наукоемкой продукции (производственные мощности, цены, технологические изменения). – М.: – ЦЭМИ РАН. – 2003. 354 стр.

5. *Варшавский Л.Е.* Использование методов теории управления для формирования рыночных структур// *Компьютерные исследования и моделирование//*– 2014. – Т. 6. – № 5. – с. 839-859.
6. *Basar T., Olsder G.J.* Dynamic Noncooperative Game Theory. – London/New York: Academic Press. – 1995.
7. *Dockner E.J., Jorgenson S. et. al.* Differential Games in Economics and Management Science. – Cambridge: Cambridge University Press. – 2000.
8. *Варшавский Л.Е.* Прогнозирование динамики показателей олигополистических рынков высокотехнологичных производств с использованием методов операционного исчисления // Труды Института системного анализа. –2019. – Т. 69.– выпуск 2. –с. 3-16
9. *Jury E.I.* Theory and Applications of the Z-Transform Method. NY. –John Wiley. –1964.
10. *Варшавский Л.Е.* Модели и методы расчета динамики ввода производственных мощностей // *Экономика и математические методы*, –1987, – т. 23, – вып. 3, – с. 456-467.

Варшавский Леонид Евгеньевич: Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Россия; Федеральное государственное бюджетное учреждение Центральный экономико-математический институт Российской академии наук» г. Москва, Россия. Главный научный сотрудник, доктор экономических наук, профессор ГАУГН. Количество печатных работ: 165 (в т.ч. 5 монографий). Область научных интересов: математическое моделирование рыночных процессов и прогнозирование показателей рынков высокотехнологичной и капиталоемкой продукции, , экономика науки. e– mail: hodvar@mail.ru

Analysis of economic indicators of oligopolistic markets under cyberthreats

L.E. Varshavsky[I,II]

[I] Federal Research Center “Computer Science and Control» of Russian Academy of Sciences, Moscow, Russia
[II] Central Economics and Mathematics Institute of Russian Academy of Sciences,, Moscow, Russia

Abstract. The article is devoted to dynamic game economic analysis of evolution of oligopolistic markets under cyber attacks on critical infrastructure. Oligopolists maximize their NPV taking into account that attacker try to minimize this criterion. Different scenarios of evolution of some abstract ologopolistic market experienced cyber attacks are considered.
Keywords: economic analysis, dynamic game, ologopolistic market, cyber attacks. *JEL Classification*: O31.
DOI: 10.14357/20790279200203

References

1. *Gordon L. A. and M. P. Loeb*. The Economics of Information Security Investment//*ACM Transactions on Information and System Security*, 2002. – pp. 438-457.
2. *Gordon L A., Loeb M. P., Zhou Lei.* Investing in Cybersecurity: Insights from the Gordon-Loeb Model// Journal of Information Security, 2016. – No7. – pp. 49-59.
3. URL: http://ceur-ws.org/Vol-2040/paper14.pdf (Access 20.11.2020).
4. *Varshavsky L.E.* 2003. Issledovanie investicionnyh strategij firm na rynkah kapitalo- i naukoemkoj produkcii (proizvodstvennye moshhnosti, ceny, tehnologicheskie izmenenija) [The study of investment strategies of firms on markets of capital and R&D intensive products].. Moscow, CEMI Russian Academy of Sciences, p. 354.
5. *Varshavsky L.E.* 2014. Ispol’zovanie metodov teorii upravlenija dlja formirovanija rynochnyh struktur [Control theory methods for creating market structures]// Komp’juternye issledovanija i modelirovani [Computer Research and Modeling]. vol. 6, no 5, pp. 839-859.
6. *Basar T., Olsder G.J.* Dynamic Noncooperative Game Theory. – London/New York: Academic Press. – 1995.
7. *Dockner E.J., Jorgenson S. et. al.* Differential Games in Economics and Management Science. – Cambridge: Cambridge University Press. – 2000.

8. *Varshavsky L.E.* 2019. Prognozirovanie dinamiki pokazatelej oligopolisticheskih rynkov vysokotehnologichnyh proizvodstv s ispol'zovaniem metodov operacionnogo ischislenija [Forecasting Dynamics of Indicators of Oligopolistic Markets of Hi-Tech Products with the help of operational calculus]//Trudy Instituta sistemnogo analiza Rossijskoj akademii nauk [Proceeding of the ISA RAS]. vol.69, no. 2: pp.3-14.
9. *Jury E.I.* Theory and Applications of the Z-Transform Method. NY. –John Wiley. –1964.
10. *Varshavsky L.E.* 1987. Modeli i metody rascheta dinamiki vvoda proizvodstvennyh moshhnostej [Models and Methods of Producrion Capacity Dynamics Planning] // Jekonomika i matematicheskie metody [Economics and Mathematical Methods]. vol. 23, no 3: pp.456-467

Varshavsky L.E. D.Sc. (Doctor of Sciences). Institute for Systems Analysis Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia; Central Economics and Mathematics Institute of Russian Academy of Sciences,, 47 Nakhimovsky prospect, Moscow 117418, Russia; e-mail: hodvar@yandex.ru. Chief scientist of the ISA RAS and of the CEMI RAS. Author of 165 articles and monographs. Fields of scientific interests: mathematical modeling of market processes and forecasting market indicators of high technology and capital intensive products, mathematical modeling of investment and innovative strategies of firms, mathematical modeling of macroeconomic processes, methods of control theory, economics of science.