ИССЛЕДОВАНИЕ ВЛИЯНИЯ КИБЕРУГРОЗ НА СТРУКТУРУ ОЛИГОПОЛИСТИЧЕСКИХ РЫНКОВ

Варшавский Л.Е.

В статье исследуется динамика показателей олигополистических рынков в условиях кибератак на производственную инфраструктуру. Участники рынка максимизируют чистую текущую стоимость (NPV) с учетом того, что целью кибератак является минимизация этого показателя. На основе динамической игровой модели проведены расчеты показателей условного олигополистического рынка при разных гипотезах о восприятии олигополистами интенсивности киберугроз.

DOI: 10.20537/mce2020econ08

1. Введение. В связи с ускоренным внедрением информационно-коммуникационных технологий (ИКТ), сопровождаемым возрастанием 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].

Из-за возрастающих киберугроз происходит непрерывный рост затрат на кибербезопасность как в государственном, так и в коммерческом секторах. В целом, во всем мире затраты на кибербезопасность в 2019 г. по оценкам компании Gartner могли составить 124 млрд долл., или 4% от всех затрат на информационно-коммуникационные технологии (ИКТ), что превышает уровень 2004 г. в 35 раз (!) [2].

Особую озабоченность вызывают участившиеся киберпреступления, направленные против критически важной инфраструктуры. Так, в последние годы отмечается рост кибератак на энергосистемы и объекты жизнеобеспечения городов и стран. На возрастающие риски поврежде-

ния своих производственных мощностей в результате кибератак все более активно указывают крупнейшие высокотехнологичные компании, такие, как, например, Intel, General Electric и др. В 2019 г. потери только российской экономики от кибератак оценивались в 1.6–1.8 трлн руб. [3].

В связи с этим, в настоящее время происходит активизация исследований в области повышения надежности киберфизических систем и их устойчивости к кибератакам. В то же время, недостаточное внимание уделяется исследованию экономических проблем, связанных с функционированием производственных и экономических систем в условиях киберугроз, особенно динамическим аспектам развития рынков, подвергающихся кибератакам. Среди небольшого числа теоретических работ, посвященных этой теме, следует отметить статьи [4, 5] и связанные с ними работы, а также [6]. 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.

Вместе с тем, ввиду того, что значительная часть продукции (особенно высокотехнологичной), а также услуг осуществляется в условиях олигополистической конкуренции (как в мире, так и в нашей стране[i]), значительный интерес представляет исследование эволюции олигополистических рынков в условиях кибератак.

Необходимо, однако, отметить, что ввиду отсутствия надежных статистических данных о числе кибератак и вызванных ими потерь (государственная статистика об этих показателях отсутствует, а данные консалтинговых организаций весьма противоречивы), возникают естественные трудности при исследовании реальных экономических процессов. В связи с этим, методические подходы и модели, которые могут быть использованы при прогнозировании таких процессов, 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

[i] Наглядным примером может служить российский рынок мобильной связи, на котором присутствуют 4 крупных компании.

инфраструктуру. Подробно исследуются методы предварительной оценки параметров игровой модели для проведения прогнозных расчетов в соответствии с различными сценариями.

2. 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 динамическая зависимость, связывающая объемы товарного производства Q_{it} со входной переменной u_{it} (вводом мощностей) и возмущением v_{it} (числом кибератак) с помощью передаточных функций $W_i(z)$ и $W_{0i}(z)$, i — индекс фирмы, $i = 1,2,...,N$, t — индекс года:

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

где z представляет 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.

Другой блок модели — обратная функция спроса, представляющая собой линейную зависимость цены на рынке P_t от объема предложения $Q_t = \sum_{i=1}^{N} Q_{it}$ (в модели предполагается баланс суммарного спроса D_t и предложения Q_t):

$$P_t = a - bQ_t, \tag{2}$$

где a, b — параметры.

Предполагается, что олигополисты используют скользящее планирование и в каждый момент времени τ максимизируют чистую теку-

щую стоимость (NPV) с учетом того, что участники кибератак стремятся нанести компаниям максимальный ущерб:

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

где: $\beta = 1/(1+r)$ — дисконтирующий множитель, соответствующий ставке дисконтирования r; P_t — цена продукции; $PL_i = (1+\mu_i)c_i + q_i / W_i(1+r_i)$ — приведенные затраты i-ой фирмы, где c_i — средние производственные издержки (без амортизации); 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, [7, 8]) 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 расчеты оптимальных по Нэшу–Курно разомкнутых (open-loop) стратегий олигополистов проведены с использованием обобщенных (generalized) матричных уравнений Риккати (см., например, [9, 10]). При этом модель (1)–(4) предварительно представлена в эквивалентной форме в пространстве состояний:

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

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

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 u_{it} линейно связаны с вектором состояния системы (5) соотношением:

$$u_{it} = K_{it} X_{t-1} + \eta_{it} \tag{6}$$

в котором K_{it} и η_{it} — векторы, зависящие от решений обобщенных уравнений Риккати [9].

3. Определение ключевых коэффициентов модели. При практическом использовании модели (1)–(3) в прогнозных исследованиях необходимо иметь адекватные оценки коэффициентов ρ_{1i} и ρ_{2i}. Для получения таких оценок могут быть полезны соотношения оптимальности, получаемые с помощью операционного исчисления (в частотной области). Так, используя этот подход к решению данной задачи, можно показать, что в случае, когда $T_p \to \infty$ [ii], при равновесии по Нэшу-Курно для задачи (1)–(3) справедливы следующие соотношения (для упрощения формул, далее принято, что $Q_{0it} \equiv 0,\ i = 1,2...N.$) (см. [8, 11]) :

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

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

где:

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

$$i = 1,2...N \tag{9}$$

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

[ii] Следует отметить, что целесообразность использования операционного исчисления обусловлена тем, что во многих случаях значения расчетных показателей при бесконечном ($T_P \to \infty$) и при конечном периоде скользящего планирования ($T_P \approx 20 \div 30$) близки.

Из (7) следует, что чем больше величина $\frac{\rho_{1i}}{\rho_{2i}}\chi_i$, 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. [12]), имеет место следующая зависимость между числом кибератак и объемом вводимых мощностей в установившемся состоянии:

$$v_{i\infty} = \lim_{z\to 1} \frac{\rho_{1i}}{\rho_{2i}}\chi_i \left[\frac{W_{0i}((\beta z)^{-1})}{W_i((\beta z)^{-1})}\right] u_{it} = CAAI_i * \left[\frac{W_{0i}(1+r)}{W_i(1+r)}\right] u_{i\infty}, \qquad (11)$$

где $\mathrm{CAAI_i} = \frac{\rho_{1i}}{\rho_{2i}}\chi_i$. В дальнейшем этот показатель будет именоваться индексом восприятия интенсивности кибератак. Очевидно в случае 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 также для определения соотношений между коэффициентами ρ_{1i} и ρ_{2i}, соответствующих желаемым оптимальным долговременным уровням товарной продукции олигополистов $Q_{i\infty}$, i=1, 2…N, Подобные задачи представляют интерес, как при прогнозировании, так и при формировании конкурентной среды государственными органами [8].

Так, ввиду (2), (8), (9) при $t \to \infty$ справедливо и:

$$P_\infty = a - bQ_\infty; \qquad (2a)$$

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

(при выводе (9а), как и (11), использовалось свойство Z–преобразования см. [12]). Из последнего соотношения можно при известных ρ_{1i} определить соотношение $\frac{\rho_{1i}}{\rho_{2i}}$ и ρ_{2i}:

$$\frac{\rho_{1i}}{\rho_{2i}} = \frac{W_i(1)W_i(1+r) - \rho_{1i}\ \Gamma_i(1,1+r)/[b(1-\Gamma_i(1,1+r)]}{\left[\chi_i^2 W_{0i}(1)W_{0i}(1+r)\right]}, i = 1,2...N; \quad (12)$$

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

В свою очередь первоначальная оценка коэффициента ρ_{1i} может быть получена из следующего соотношения, связывающего средний допустимый для i-го олигополиста уровень ввода мощностей (производственных инвестиций) со средней предполагаемой ценой $\bar{P}$:

$$\bar{u_i} = \frac{W_i(1+r)(\bar{P} - PL_i)}{\rho_{1i} + b\left[W_i(1)W_i(1+r) - \frac{\rho_{1i}}{\rho_{2i}}\chi_i^2 W_{0i}(1)W_{0i}(1+r)\right]} = \quad (14)$$

$$= \frac{W_i(1+r)(\bar{P} - PL_i)}{\rho_{1i}\left[1+\Gamma(1,1+r)/(1-\Gamma(1,1+r))\right]} = \frac{W_i(1+r)(\bar{P} - PL_i)(1-\Gamma(1,1+r))}{\rho_{1i}}.$$

(второе равенство в (14) следует из (9а)). Из (14) можно получить оценку ρ_{1i}:

$$\rho_{1i} = \frac{W_i(1+r)(\bar{P} - PL_i)(1-\Gamma(1,1+r))}{\bar{u_i}}, \quad (14a)$$

которую можно применить для вычисления ρ_{2i}. Далее, используя соотношение (7), можно получить оценку средней интенсивности кибератак $\bar{v}_i$. Если она не согласуется с ожидаемой интенсивностью, то следует провести корректировку задаваемого значения $\bar{v}_i$ и далее, на основе (13)–(14), (14а) — коэффициентов ρ_{1i} и ρ_{2i}.

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. В частности, могут быть исследованы стратегии атакующих, заключающиеся в снижении интенсивности кибератак при одновременном повышении эффективности каждой атаки (например, за счет повышения вредоносного трафика и увеличения задействованного оборудования в каждой атаке). При этом следует иметь в виду достаточно высокую чувствительность результатов расчетов от принимаемой величины периода скользящего планирования T_p (см. п. 4.2).

4. Результаты расчетов. На условном примере триополии ниже рассматриваются изложенные выше подходы к прогнозированию динамики показателей олигополистических рынков при наличии кибератак на производственную инфраструктуру. В качестве центрального блока модели рассматривается, модель освоения мощностей [13], для которой соотношения типа (1) для каждого олигополиста в пространстве состояний могут быть представлены в виде:

$$X_{it} = A_i X_{it-1} + B_i u_{it} + D_i v_{it}, \tag{15}$$

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

$$A_i = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & \lambda \end{pmatrix}; \quad \mathrm{B_i} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}; \quad \mathrm{D_i} = \begin{pmatrix} 0 \\ 0 \\ -\chi_i \end{pmatrix} \tag{16}$$

$$Q_{it} = (k_0, k_1, 1) X_{it}, 0 < k_0 < k_1 < 1, i = 1, 2, ..., N.$$

В базовом варианте 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 табл. 1.

Таблица 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	3.0

Таким образом, в базовом варианте третья компания, имеющая лучшие экономические показатели (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: $a = 160$: $b = 0{,}15$, а $\lambda = 0.75$.

4.1. Прогнозирование при постоянных значениях индексов $\mathrm{CAAI_i}$**.** В данном случае принимаемая гипотеза состоит в том, что олигополисты при разработке стратегий развития исходят из предположения о стабильной относительной интенсивности атак (при этом индекс $\mathrm{CAAI_i} = \dfrac{\rho_{1i}}{\rho_{2i}}\chi_i$ остается постоянным даже при уменьшении вероятности успешных атак $p(\mu_i)$ и соответственно при росте затрат на кибербезопасность μ_i).

Расчеты при следующих значениях индексов восприятия интенсивности атак: $\mathrm{CAAI_i} = 2.204, i = 1,2; \mathrm{CAAI_3} = 2.256$ показывают, что увеличение доли затрат компаний на кибербезопасность от OPEX до 0.07–0.08 приводит к росту всех ключевых экономических показателей, что, в частности, отражается на увеличении показателей чистой текущей стоимости (NPV) в компаниях. Дальнейший рост доли затрат приводит к

снижению объемов производственных инвестиций и производства, а также показателей эффективности. 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 (см. рис. 1–2). Таким образом, несмотря на снижение показателя NPV после увеличения доли затрат на кибербезопасность относительно оптимального уровня (для компании-лидера он составляет 8%), происходит некоторое изменение рыночной структуры в сторону повышения рыночной доли наиболее эффективной третьей компании.

Интересно отметить также стабилизацию отношения интенсивности атак к вводу мощностей v_{3t}/u_{3t} для всех компаний, что согласуется с (11). Так, например, для компании-лидера динамика этого отношения постепенно стабилизируется на уровне 1.825, что соответствует теоретическому значению, определяемому по формуле (11) (рис. 3).

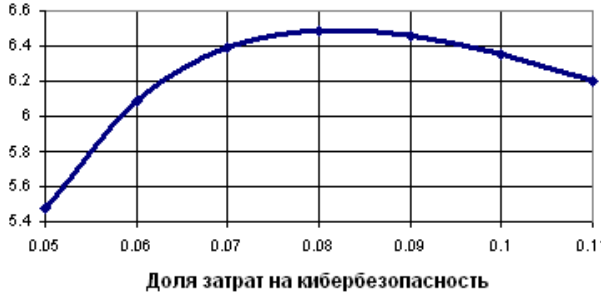

Рис. 1. Зависимость показателя NPV за 20 лет (млн усл. ед.) третьей компании в триополии от доли затрат μ на кибербезопасность при $\mathrm{CAAI}_i = const$.

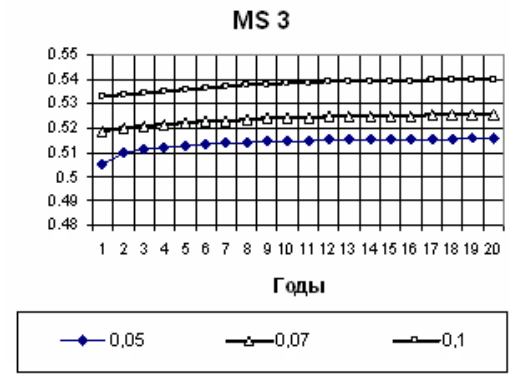

Рис. 2. Динамика рыночной доли третьей компании (MS 3) в триополии при разных долях затрат на кибербезопасность μ (μ=0.05; 0.07; 0.10).

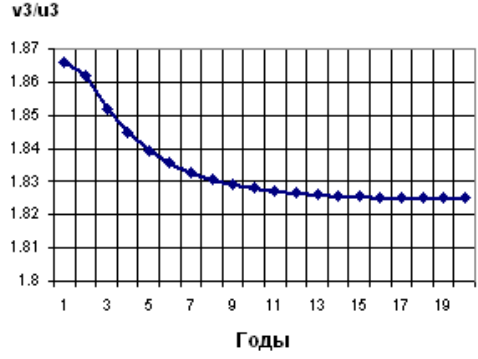

Рис. 3. Динамика отношения интенсивности атак к вводу мощностей v_{3t} / u_{3t} в третьей компании (μ=0.07).

4.2. Прогнозирование при изменяющихся во времени значениях коэффициентов. В случае, когда участники рынка руководствуются гипотезой о переменных во времени значениях коэффициентов ρ_{2it} u $g_{it}; i = 1,2,3$, справедливо лишь соотношение (7). При этом, как отмечалось выше, продолжительность периода скользящего планирования T_p в (3) существенно влияет на динамику расчетных экономических по-

казателей. Так, на рис. 4 приведена динамика суммарных объемов товарной продукции при продолжительности периода скользящего планирования T_p у олигополистов, равной 10, 20, 50 лет, и при постоянных темпах роста коэффициентов ρ_{2it} u $g_{it}; i = 1,2,3$, соответственно $\delta g_{it} = 1.025$ и $\delta\rho_{i2t} = 1.035$ (остальные параметры модели соответствуют базовому варианту).

Расчеты, проведенные при разных темпах роста коэффициентов ρ_{2it} u $g_{it}; i = 1,2,3$ (табл. 2) для базового варианта при $T_p = 20$ годам, показывают, что для стабилизации объемов товарной продукции необходимо существенное превышение темпов роста коэффициента восприятия интенсивности кибератак $\delta\rho_{2it}$ над темпами роста коэффициента потерь δg_{it}, т.е. $\delta\rho_{2it} > \delta g_{it}; i = 1,2,3$. При равенстве этих темпов (в данном примере при $\delta\rho_{2it} = \delta g_{it} > 1.01;\ i = 1,2,3$) к концу прогнозного периода не происходит компенсации экспоненциально возрастающих потерь (рис. 5).

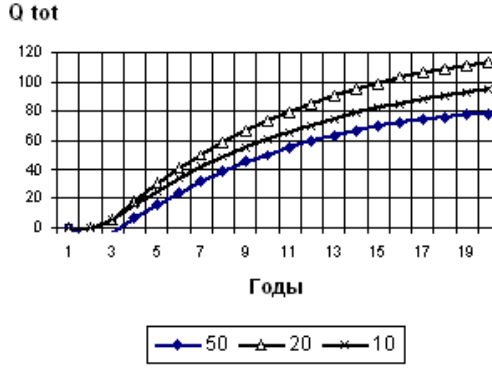

Рис. 4. Динамика суммарных объемов товарной продукции (Q_{tot}, тыс. усл. ед.) в триополии при разной продолжительности периода скользящего планирования T_p.

Таблица 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	1.025	1.035
2	1.035	1.045
3	1.035	1.035

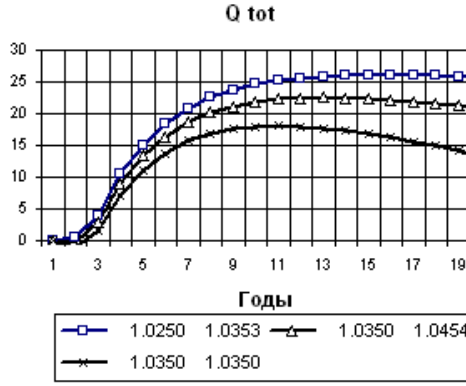

Рис. 5. Динамика суммарных объемов товарной продукции (Q_{tot}, тыс. усл. ед.) в триополии при разных темпах роста величины ущерба от одной атаки δg_i и коэффициентов $\delta\rho_{2i}$ i=1,2,3.

4.3. Прогнозирование с учетом стремления олигополистов обеспечить себе желаемые доли на рынке. В этом случае предполагается, что в долгосрочной перспективе олигополисты стремятся обеспечить следующие объемы выпуска товарной продукции: $Q_{1\infty} = Q_{1\infty} = 25$ и $Q_3 = 70$ тыс. единиц. Ниже проведены результаты расчетов для двух вариантов с равными объемами желаемой товарной продукции, но различающихся допустимыми уровнями средних объемов ввода мощностей $\overline{u_i}$ и соответственно значениями коэффициентов ρ_{1i}, ρ_{2i} i=1,2,3 (табл. 3а, 3б). Значения остальных параметров модели (1)–(3) приняты такими же, как и в базовом варианте.

Вариант 2, характеризующийся существенно большими значениями отношений ρ_{1i} / ρ_{2i}, соответствует значительному росту интенсивности кибератак и, как следствие этого, инвестиций, что связано с необходимостью компенсации большего ущерба из-за дополнительных потерь, вызываемых большим числом атак (рис. 6,7). Значение показателя NPV за 20 лет во втором варианте заметно ниже, чем в первом (табл. 4). Вместе с тем, расчеты показывают, что при отсутствии кибератак значение показателя эффективности NPV для первых двух компаний составило бы 5.1 млн усл. ед., а для третьей — 26.0 млн усл. ед., что соответственно на 43% и 29% выше, чем в варианте 1.

Таблица 3а. Допустимые уровни средних объемов ввода мощностей $\bar{u}_i$ в вариантах 1 и 2.

Вариант 1		Вариант 2	
$\bar{u}_1 = \bar{u}_2$	$\bar{u}_3$	$\bar{u}_1 = \bar{u}_2$	$\bar{u}_3$
7	18	8	21

Таблица 3б. Значения коэффициентов ρ_{1i}, ρ_{2i} в вариантах 1 и 2.

Вариант	$\rho_{11} = \rho_{12}$	$\rho_{21} = \rho_{22}$	ρ_{13}	ρ_{23}
1	10.24	6.02	6.11	0.80
2	8.96	0.73	5.24	0.28

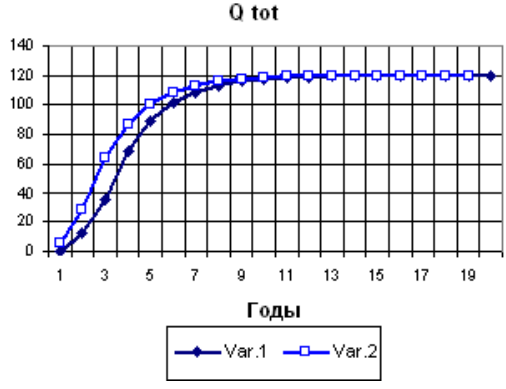

Рис. 6. Динамика суммарных объемов товарной продукции (Q_{tot}, тыс. усл. ед.) в триополии при разных допустимых уровнях средних объемов ввода мощностей $\bar{u}_i$.

Таблица 4. Расчетные значения показателей NPV компаний, млн усл. ед.

Вариант	NPV 1, 2	NPV 3
1	3.58	20.19
2	2.26	15.51

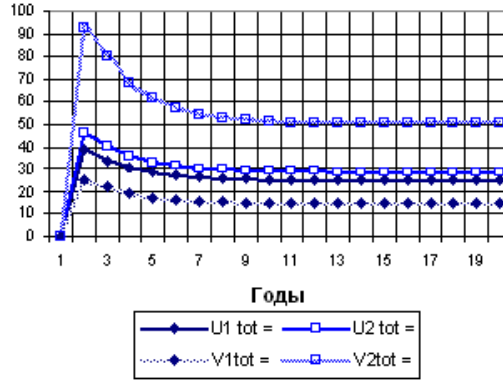

Рис. 7. Динамика суммарных объемов ввода мощностей (U_{tot}, тыс. ед.) и интенсивностей кибератак (V_{tot}, тыс.) в триополии при разных допустимых уровнях средних объемов ввода мощностей $\bar{u}_i$.

Выводы. Рассмотренный игровой подход позволяет получить предварительные оценки целесообразных затрат на кибербезопасность для участников олигополистических рынков, а также разрабатывать сценарии поведения участников рынка на основе различных гипотез об интенсивности и эффективности кибератак.

Использование операционного исчисления существенно упрощает формирование гипотез, закладываемых в основу различных прогнозных сценариев развития рынков.

СПИСОК ЛИТЕРАТУРЫ

1. Cybercrime ‘pandemic’ may have cost the world $600 billion last year / CNBC. URL: https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html.
2. Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. URL: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.

3. Хакеры похоронили «Цифровую Россию»: Кибермошенники атакуют страну каждые 10 минут. URL: http://www.ng.ru/economics/2019-11-05/1_7718_hakers.html.
4. *Gordon, L. A. and M. P. Loeb*. The Economics of Information Security Investment//*ACM Transactions on Information and System Security*, 2002. P. 438-457.
5. *Gordon L A., Loeb M. P., Zhou Lei*. Investing in Cybersecurity: Insights from the Gordon-Loeb Model // *Journal of Information Security*, 2016. No7. P. 49-59.
6. *Alexeev A., Jardine E., Krutilla K.* Optimal Investment in Cyber Attack and Resilience: A Dynamic Differential Game. URL: http://ceur-ws.org/Vol-2040/paper14.pdf.
7. *Варшавский Л.Е*. Исследование инвестиционных стратегий фирм на рынках капитало- и наукоемкой продукции (производственные мощности, цены, технологические изменения). – М.: ЦЭМИ РАН. 2003. 354 стр.
8. *Варшавский Л.Е.* Использование методов теории управления для формирования рыночных структур // *Компьютерные исследования и моделирование.* 2014. Т. 6. № 5. с. 839–859.
9. *Basar T., Olsder G.J.* Dynamic Noncooperative Game Theory. London/New York: Academic Press. 1995.
10. *Dockner E.J., Jorgenson S. et. al.* Differential Games in Economics and Management Science. Cambridge: Cambridge University Press. 2000.
11. *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.
12. *Jury E.I.* Theory and Applications of the Z-Transform Method. NY. John Wiley, 1964.
13. *Варшавский Л.Е.* Модели и методы расчета динамики ввода производственных мощностей // *Экономика и математические методы.* 1987. Т.23, вып. 3. С. 456-467.

STUDYING INFLUENCE OF CYBERTHREATS ON ECONOMIC INDICATORS OF OLIGOPOLISTIC MARKETS

Varshavsky L.E.

Dynamics of economic indicators of oligopolistic markets under cyber attacks on critical infrastructure is studied. Oligopolists maximize their NPV taking into account that attacker try to minimize this criterion. Scenarios of evolution of some abstract oligopolistic market under cyber attacks are considered.