UDC 621.52+511.52

# MODELING THE IMPACT OF RISK ON CYBERSECURITY INVESTMENT PROJECTS

**A.H. Grigoryan**

*National Defense Research University, Ministry of Defense, Armenia*

Investment decision-making under ambiguity is a complex process, which becomes more compound in terms of the stochastic nature of cyber environment. Therefore, development of robust models is needed to address the dynamic nature of cyber threats and various types of risks existing in cybersecurity investment projects. The recent research in cybersecurity investments shows, that the most frequently used model targeted at analysing investments is the Gordon-Loeb investment model. The article presents a model for cybersecurity investment decision-making under ambiguity by the extension of the Gordon-Loeb investment model based on real options. In this paper, under deep uncertainty and various types of risks in cyber environment, cybersecurity threats are modeled as stochastic processes under ambiguity using the Choquet-Brownian motions. Given the ambiguity existing in cyber environment, it is drastically important to consider the impact of risks on the cybersecurity investment projects. The aim of our research is to analyze the possible scenarios, regarding the impact of risks and ambiguity on the cybersecurity investment projects. Our work has led us to conclude, that considering the compound interconnections between risks and uncertainty will give decision-makers an opportunity to effectively address the stochastic nature of cybersecurity investments and make optimal decisions.

***Keywords:*** cybersecurity, modeling, real option, Choquet-Brownian motion, investment, risk, ambiguity.

***Introduction.*** An information system is characterized by three parameters: the monetary losses $\lambda$ in case a cybersecurity breach occurs, the threat probability $\xi$ and the inherent vulnerability $\upsilon$, denoting the probability that without additional security, a realized threat is successful. In Gordon-Loeb model, the expected losses $L$ associated with the threat against the information system, are calculated as $L = \xi\lambda$, where $\xi$ is the probability of the threat occurred and $\lambda$ is the monetary losses. To reduce the vulnerability $\upsilon$ of an information system, an organization invests $(z > 0)$ monetary units. In this respect, $S(z, \upsilon)$ represents the remaining vulnerability [1-3].

Taking into account the complex and stochastic nature of cybersecurity threats and the ambigous characteristics of cyber environment, uncertainty in cybersecurity threats is introduced inside the model through the use of Choquet-Brownian motions [4].

Let's consider an increase in ambiguity, which is a deviation from neutral case $(c = 1/2)$ for the Choquet-Brownian setting. In this case, $\Psi$ will represent the index of intensity (degree) of ambiguity ($\Psi$-ignorance), which is similar to the index $k$ in the multiple-priors model ($k$-ignorance) [5]. In this regard, $\Psi$ depends on parameter $c$, so that $\Psi = 0$, when $c = 1/2$ (special case of the absence of ambiguity). Thus, $\Psi = \frac{1}{2} - c$ with $\Psi = \left[-\frac{1}{2}, \frac{1}{2}\right]$. For example, when the decision-maker is ambiguity averse, then $c < \frac{1}{2}, \Psi > 0$.

Taking into account the above-mentioned statements, the impact of risk and ambiguity on the cybersecurity investment project will be discussed in the following sections.

***Impact of Risk.*** To discuss the effects of risk (volatility) on the value and optimal timing of the cybersecurity investment project, let us represent the risk $\boldsymbol{\sigma^2}$.

In this case, if there is no ambiguity and the decision-maker is risk neutral, then $(m = 2c - 1 = 0)$ and consequently $W(\pi_t) = \frac{\pi_t}{\rho - \mu}$. This means, that a change in risk does not modify the value of the cybersecurity investment project in the stopping region.

Further, equations (1), (2), and (3) will be used for modeling the impact of risk on the cybersecurity invest project:

$$W(\pi_t, t) = \int_t^T \pi_t \exp(-(\rho - \mu)(s - t)ds) == \frac{\pi_t}{\rho - \mu}\left(1 - e^{-(\rho-\mu)(T-t)}\right), \quad (1)$$

$$W(\pi_t) = \frac{\pi_t}{\rho - \mu}\ , \quad (2)$$

$$W(\pi_t) = \frac{\pi_t}{\rho - (\mu + m\sigma)}\ . \quad (3)$$

Now, let's consider the impact of risk on the changes in continuation region and on the reservation value. Regarding the option value in the continuation region, $V(W_t)$ will be presented by the following expression:

$$V(W_t) = \left(\frac{z}{a-1}\right)^{1-a} a^{-a} W_t^a\ ,\quad W_t < W^*\ . \quad (4)$$

In this case, the parameter $\sigma^2$ plays a significant role for computation of $a$:

$$a = \frac{-\left((\mu + m\sigma) - \frac{1}{2}(s\sigma)^2\right) + \sqrt{\left\{(\mu + m\sigma) - \frac{1}{2}(s\sigma)^2\right\}^2 + 2\rho(s\sigma)^2}}{(s\sigma)^2}. \quad (5)$$

Taking into account what was discussed above, the change in risk will modify the value of the cybersecurity project in the continuation region. In this connection, identification of the impact of an increase in risk depends on the sign of a derivatives presented below [4, 6]:

$$\begin{cases} \frac{\partial a}{\partial \sigma^2} < 0 \ , \\ \frac{\partial V(W_t)}{\partial a} < 0 \ . \end{cases} \tag{6}$$

The calculations show, that $\frac{\partial V(W_t)}{\partial \sigma^2} > 0$, thus, an incraese in risk increases the value of the cybersecurity project in the contination region.

The parameter $\sigma^2$ has the same impact on the reservation value represented below:

$$W^* = \frac{a}{a-1} z \ . \tag{7}$$

Like continuation region, the identification of the impact of an increase in risk depends on the sign of a derivatives presented below [4, 6]:

$$\begin{cases} \frac{\partial W^*}{\partial a} < 0 \ , \\ \frac{\partial a}{\partial \sigma^2} < 0 \ . \end{cases} \tag{8}$$

Hence, $\frac{\partial W^*}{\partial \sigma^2} > 0$, which means that an increase in risk increases the reservation value of the cybersecurity investment project. This makes it possible to establish a connection between the change in reservation value and the consequent impact on timing of option exercise. By reinterpreting the reservation value $W^*$ in terms of reservation threat of the attempted breach $\xi^*$, from (3) we get:

$$W^* = \frac{\pi^*}{\rho-(\mu+m\sigma)} = \frac{(v-S(z-v))\lambda\xi^*}{\rho-(\mu+m\sigma)} \ . \tag{9}$$

In this connection, when the current thraet $\xi < \xi^*$, then the value of $W_t < W^*$ and from (8) we have:

$$\xi^* = \frac{W^*(\rho-(\mu+m\sigma))}{(v-S(z-v))\lambda} \ . \tag{10}$$

Since, in the Gordon-Loeb model [1, 2] $\big(v - S(z - v)\big)\lambda$ is independent of time, this allows to conclude that waiting until $\xi$ exceeds $\xi^*$ remains the optimal cybersecurity investment strategy, and it holds true until:

$$\left(\rho - (\mu + m\sigma)\right) > 0\,. \tag{11}$$

Thus, in the absence of ambiguity, an increase in risk leads to the increase in the value of the cybersecurity investment project in the continuation region $W_t$ and in the reservation value $W^*$, without changing the value of the project once the option has been exercised.

Now, let us consider the case when ambiguity is introduced in the form of Choquet distortion with Choquet-Brownian motions. In this connection, if $\sigma^2$ increases, $(\mu + m\sigma)$ increases if and only if $m > 0$, that is, if $c > \frac{1}{2}$ and $\Psi < 0$, as $\Psi = \frac{1}{2} - c$. This in its turn implies, that $W(\pi_t) = \frac{\pi_t}{\rho - (\mu + m\sigma)}$ increases as well. Consequently, if the decision-maker is ambiguity-lover the cybersecurity investment project value in the stopping region also increases with the increase in risk. In the same manner, if the decision-maker is ambiguity averse, the cybersecurity investment project value in the stopping region decreases, which means, that $c < \frac{1}{2}$.

It should be also noted, that in case of multiple-priors, when $k > 0$, in the presence of ambiguity an increase in risk leads to a decrease in the value of cybersecurity investment project, as $W_t = \frac{\pi_t}{\rho - (\mu + m\sigma)}$ , which is a special case of Choquet-Brownian motion model.

Overall, the presence of ambiguity appears to be sufficient to intoduce an impact of risk on the exercised cybersecurity investment project value, while in the standard case of an absence of ambiguity it was not modified. It is very important to note that differences in original attitude towards ambiguity may explain why the same variation in risk may be looked over differently by decision-makers, revealing different attitudes towards perceived ambiguity, with potentially drastic consequences in terms of valuation. So, in the presence of ambiguity, a change in risk impacts the project value in the stopping region, depending on the decision-maker's preferences towards ambiguity. An increase in risk leads to an increase in the value of the cybersecurity investment project once the option has been exercised, if and only if the decision-maker is ambiguity lover $\left(c > \frac{1}{2}\right)$. The opposite holds true, if the decision-maker is ambiguity-averse to $\left(c < \frac{1}{2}\right)$.

***Conclusion***. Taking into account the complex and stochastic nature of cybersecurity threats and the ambigous characteristics of cyber environment, it is

drastically important for decision-makers to consider the impact of risk on the cybersecurity investment projects.

In this connection, analysis of possible scenarios regarding the impact of risks on the investment projects will lead to the consideration of the compound interconnections between risks and ambiguity in cyber environment and make optimal investment decisions.

**References**


1. **Gordon L.A., Loeb M.P.** The Economics of Information Security Investment // ACM Transactions on Information and System Security. - 2002. - Vol. 5, N. 4. - P. 438-457.
2. **Gordon L.A., Loeb M.P.** Managing Cybersecurity Resources: A Cost-Benefit Analysis. The Mcgraw-Hill Homeland Security Series. - 2006. - 224 p.
3. **Demetz L., Bachlechner D.** To Invest or Not to Invest? Assessing the Economic viability of a Policy and Security Configuration Management Tool // The Economics of Information Security and Privacy, Springer. - 2013. - P. 25-47.
4. **Roubaud D., Lapied A., Kast R.** Real Options under Choquet-Brownian Ambiguity // HAL. halshs-00534027, - 2010.
5. **Chen Z., Epstein L.G.** Ambiguity, Risk, and Asset Returns in Continuous Time // Econometrica. - 2002. –Vol. 70, N. 4. - P. 1403-1443.
6. **Nishimura K.G., Ozaki H.** Irreversible Investment and Knightian Uncertainty // Journal of Economic Theory. – 2007. – Vol. 136, N. 1. – P. 668–694.



*Received on 25.09.2017.*
*Accepted for publication 21.12.2017.*


## ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ՈԼՈՐՏՈՒՄ ՆԵՐԴՐՈՒՄԱՅԻՆ ՆԱԽԱԳԾԵՐԻ ՎՐԱ ՌԻՍԿԻ ԱԶԴԵՑՈՒԹՅԱՆ ՄՈԴԵԼԱՎՈՐՈՒՄԸ


**Ա.Հ. Գրիգորյան**



Խոր անորոշության պայմաններում ներդրումային վճիռների կայացումը՝ որպես բարդ գործընթաց, էլ ավելի է բարդանում կիբեռմիջավայրին բնորոշ ստոխաստիկության պայմաններում: Ոչստի կիբեռսպառնալիքների դինամիկական բնույթի և կիբեռանվտանգության ոլորտում ներդրումային նախագծերում առկա տարբեր տեսակի ռիսկերի դիտարկման համար անհրաժեշտ է մշակել ռոբաստ մոդելներ: Կիբեռանվտանգության ոլորտում կատարվող ներդրումներին վերաբերող հետազոտական աշխատանքներում առավել հաճախ կիրառվում է Գորդոն-Լոեբի ներդրումային մոդելը: Ներկայացված է Գորդոն-Լոեբի ներդրումային մոդելի ընդլայնմամբ իրական օպցիոնների վրա հիմնված մոդել՝ խոր անորոշության պայմաններում կիբեռանվտանգության ոլորտում ներդրումային վճիռների կայացման համար: Հաշվի առնելով կիբեռսպառնալիքների բարդ և ստոխաստիկ բնույթը, ինչպես նաև կիբեռմիջավայրում առկա խոր անորոշությունը՝ շոկե-

բրոունյան շարժման միջոցով մեր կողմից մոդելավորվել են կիբեռսպառնալիքները՝ որպես ստոխաստիկ պրոցեսներ խոր անորոշության պայմաններում: Կիբեռմիջավայրում առկա խոր անորոշության պայմաններում վճիռ կայացնելու համար խիստ կարևոր է դիտարկել ռիսկի ազդեցությունը կիբեռանվտանգության ոլորտում ներդրումային նախագծերի վրա: Հետազոտության նպատակն է կիբեռանվտանգության ոլորտում ներդրումային նախագծերի վրա ռիսկի և անորոշությամբ պայմանավորված իրավիճակների ազդեցության հնարավոր սցենարների վերլուծությունը: Մեր կողմից կատարված հետազոտական տվյալների մշակմամբ կարելի է եզրահանգել, որ ռիսկերի և անորոշության միջև առկա բարդ փոխկապվածության հաշվառումը վճիռ կայացնողին հնարավորություն կտա արդյունավետ կերպով դիտարկելու կիբեռանվտանգության ոլորտում ներդրումային նախագծերի ստոխաստիկ բնույթը և կայացնելու օպտիմալ վճիռներ:

***Առանցքային բառեր.*** կիբեռանվտանգություն, մոդելավորում, իրական օպցիոն, շոկե-բրոունյան շարժում, ներդրում, ռիսկ, խոր անորոշություն:

## МОДЕЛИРОВАНИЕ ВОЗДЕЙСТВИЯ РИСКА НА ИНВЕСТИЦИОННЫЕ ПРОЕКТЫ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

**А.Г. Григорян**

Принятие инвестиционных решений в условиях глубокой неопределенности, являясь довольно сложным процессом, становится более сложным в стохастических условиях, которые характерны для киберсреды. В связи с этим для исследования динамического характера киберугроз и различных видов рисков в инвестиционных проектах в сфере кибербезопасности необходимо разработать робастные модели. В исследованиях, направленных на анализ инвестиций в сфере кибербезопасности, часто применяется инвестиционная модель Гордона-Лоэба. В статье на основе реальных опционов представлена расширенная инвестиционная модель Гордона-Лоэба, характеризующая принятие инвестиционных решений в условиях глубокой неопределенности. Путем применения шоке-броуновского движения смоделированы киберугрозы как стохастические процессы в условиях глубокой неопределенности с учетом сложного и стохастического характера киберугроз, а также фактора глубокой неопределенности в киберсреде. При принятии решения в условиях глубокой неопределенности в киберсреде существенным является изучение воздействия риска на инвестиционные проекты в кибербезопасной среде. Цель исследования – провести анализ возможных сценариев влияния риска и различных ситуаций, обусловленных неопределенностью, на инвестиционные проекты в сфере кибербезопасности. Исходя из анализа результатов данных исследований, можно сделать вывод о том, что учет сложной взаимосвязи между риском и неопределенностью дает возможность для лица, принимающего решение, более эффективно рассмотреть стохастический характер инвестиционных проектов в сфере кибербезопасности и принять оптимальные решения.

***Ключевые слова:*** кибербезопасность, моделирование, реальный опцион, шоке-броуновское движение, инвестиция, риск, глубокая неопределенность.