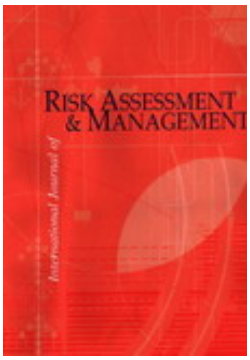


International Journal of Risk Assessment and Management

ISSN online: 1741-5241 - ISSN print: 1466-8297
https://www.inderscience.com/ijram

On the black swan risk dynamical evaluation

Sergei Zuev, Petr Kabalyants

DOI: 10.1504/IJRAM.2022.10053796

Article History:

Received:	26 July 2020
Accepted:	08 January 2021
Published online:	02 February 2023

On the black swan risk dynamical evaluation

Sergei Zuev* and Petr Kabalyants

Department of Computer Science,
Belgorod Shoukhov State University of Technologies,
Belgorod, 308012, Russia
Fax: +7 4722 557139
Email: sergey.zuev@bk.ru
Email: kabalyants@gmail.com
*Corresponding author

Abstract: The paper was inspired by comprehensive researches in the field of video data information security. Video data is considered as a long range of frames. This work is targeted on the problem of correlations between the already happened and upcoming incidents in terms of their probability. The main idea of the paper is to take into account some hidden events that provoke the incidents. The possible incident is modelled as a finite sequence of those events. The statistical ensemble approach is used in order to evaluate an incident probability if there were no registered incidents in the system yet. It is shown that the probability can be evaluated dynamically if there is enough data about previous incidents in the statistical ensemble. Thus, it is supposed that the risk manager can operatively gather information from the similar information systems.

Keywords: black swan; risk evaluation; dynamical risk evaluation; Weibull distribution; computer aided risk evaluation; information risk assessment.

Reference to this paper should be made as follows: Zuev, S. and Kabalyants, P. (2022) 'On the black swan risk dynamical evaluation', *Int. J. Risk Assessment and Management*, Vol. 25, Nos. 1/2, pp.56–66.

Biographical notes: Sergei Zuev received his PhD in Geometry and Topologies at Kazan University. He is an Associate Professor at the Department of Computer Science, Belgorod Shoukhov University of Technologies. His research interests include issues related to conceptual uncertainty in information security and reliability theory, quantum computing and neural networks in the field of artificial intelligence and newest computational methods. He has published research papers in national and international journals, conference proceedings, textbooks as well as industrial research projects.

Petr Kabalyants received his PhD in Mathematical Modelling and Computational Mathematics at Kharkiv National University of Radio Electronics. He is an Associate Professor at the Department of Computer Science, Belgorod Shoukhov University of Technologies. His research interests are related to machine learning, image recognition, probability theory and reliability theory. He has published research papers in national and international journals, conference proceedings, textbooks as well as book chapters.

This paper is a revised and expanded version of a paper entitled 'Probability model of risk' presented at International Conference *"Modeling Analysis of Security and Risk in Complex Systems"*, St. Petersburg, Russia, 23–25 June, 2020.

1 Introduction

Rare incidents with significant impact in the field of information security have lack of studies today. The main reason is that they say "there are very few known incidents of that type in cybersecurity at all" (Astahov, 2010). However, any zero day vulnerability brings such kind of risk (Taleb, 2007). The APT and other kinds of attacks, that usually seem to occur in a specific company rather unlikely, can be concerned as an appointed threat as well. The artificial random threats, that bring more than a half of total harm of information security incidents, could be added to the set of such threats. It is more likely that the very information risk management is the main reason to avoid black swans consideration in cybersecurity. Because risk managers deal with quite a long-time period of risks validation that is determined by corporate management, expert re-assessments require resources and they are forced to be as rare as possible.

The risk definition implies multiplication of two factors: an evaluation of possible damage and a threat incident probability. Both factors have a great deal of uncertainty, that is connected to complexity of the system. This complexity implies that there are a lot of hidden parameters in the system and, of course, any parameter may change its value over time. The consequences are significant fluctuations of the risk value that forces to perform reassessment. In order to break uncertainty, it is common to use expert assessments and to form as large a pool of experts as possible. This, of course, exploits the ergodic hypothesis. At the same time, due to the openness of real systems, there are big obstacles to apply the ergodic hypothesis here. A large number of modern research methods exploit ergodicity (van Handel, 2014). In this regard, there is a great temptation to describe non-ergodic systems by some ergodic tools and methods.

In the present paper we propose a theoretical background for a risk probability distribution derivation. The corresponding technique is presented.

1.1 Incident model and data mining

At first, we make a model that describes an incident genesis. Of course, nobody knows how an incident occurs definitely. But based on some natural proposition or just intuition, we can suppose that there are some events that precede incident and increase its probability. Moreover, we should suppose that the incident occurs just in specific case, when there are more than a fixed number of events occur during some fixed time. The natural question is: how to gain information on these causing events when we have no idea what kind of events are meant? The answer is given afterwards. Suppose that the incident happened already, but not in the controlled system, and we have information about the incident. Assume also that there is a known pool of the systems similar to our system and we can observe them and receive operative information from them. This situation is becoming more real every day because more and more people understand the importance of the data sharing. In this case we have some kind of statistical ensemble and we can proceed with statistical data although we have no any incidents in our system.

There is a wide range of possible data to collect: incidents after personnel errors, random technical accidents, zero-day vulnerability finding and/or exploiting, grid system crashing by undisclosed reason and so on. All that may cause big damage and, of course, can be treated as black swans. Various ways to collect data may be used: internet sites parsing, queries to special databases, regular requests to news agencies and so on. These forms are often used, but there are a lot of additional possible ways to collect data. For further consideration we suppose that the data have been already collected and the way of their collection is determined. However, in real cases, the choice between several data collection methods may present a big challenge.

1.2 Data formats and structures

We use Python for the data processing. Of course, there are no restrictions for other tools, but in order to express what kind of data types we use, it is better to clarify the language. The collected data has to be presented as lists or DataFrames in order to simplify further processing. The data must contain the follow information at least: number, type and time of the incident, an identification number of the system where incident occurred, the scale factor for the system to be compared to target system.

We suppose that incident probabilities and the corresponding damages are rather independent values. Because the same incident may cause very different consequences in different systems or even in the same system, but in different times, our approach concerns just probabilities and does not involve possible damage re-evaluation. The reason is that damage can be re-evaluated when there are some changes in assets or it can be evaluated periodically, for instance, one or two times per year; there is no any connection between damage evaluation and already happened incidents.

Another parameter that should be taken into account is the data freshness: if an incident occurs somewhere in observable ensemble of systems, then we should know about it as soon as possible. In case if the delay becomes more than its limit value, then there is no any sense to make risk evaluation because there is no chance to take an action. That is why any received data has to be marked by the renewal time. This time does not coincide with the last incident detection time because we have chance to detect no incidents for a long time of the observations.

For our further considerations we use the data in the following simplified form:

$$x_1, x_2, \ldots,$$

where every value x_i may be just 0 or 1 that corresponds to the cases "no incident" or "incident" respectively. However, this sequence is not Bernoulli's type because we have, in general, various probabilities for 0 and 1 at the specified i, i.e., the sequence is not stationary. Further we suppose that every x_i resulted from some finite series of Bernoulli type and this is core idea of our consideration.

Of course, in order to evaluate the target system risk, it is necessary to have the scale factor between the target system and the whole observable ensemble. We suppose that the scale factor is known and denote it as $\sigma < 1$. The indices i in the notation x_i correspond to the observations number and it is assumed that any observation takes a constant time τ. Thus, we have Bernoulli sequence $\xi_1, \xi_2, \ldots$ of undisclosed events and it is equal-interval time series. In our simplified formulation, the mentioned outcomes x_i are resulted from some subsequences of the sequence $\{\xi_j\}$.

1.3 Our contribution

We bring to the risk evaluation toolkit a new technique for the assessment of short-time risk value enhancing and the duration of the enhanced risk. This contribution makes it possible to manage risk while it essentially increases for a short time if the risk manager has some pool of possible actions that can be activated on demand. The protection of such type looks like a "fire shield", but in the considered cases the company does not buy this shield but just rent it. An ability to make appointed assessments in the background mode can be treated as an advantage of proposed technique.

2 Finite series probability space

Let us consider a Bernoulli sequence $\xi_1, \xi_2, \ldots$ of some events with p as probability for outcome 1, that corresponds to above mentioned causing event. Let $\eta_i^k = \{\xi_i, \ldots, \xi_{i+k-1}\}$ be a finite series of k elements from the sequence, starting from the ith element $\xi_i = 1$. We call the series η_i^k simply as *k-series*. We define a special kind of k-series with at least a outcomes 1 inside and we call them *a-positive k-series*.

While we model an incident as a result of some sequence of events, we should turn to the conception of the *Markov breakpoint* introduced in (Shiryaev, 1996) monograph as *stopping time*. In the considered case the Markov breakpoint takes place on the following criterion: during a certain time preceding the breakpoint, there are at least a fixed number a of causing events. In case of number of events less than a, the breakpoint does not occur. An incident corresponds to the Markov breakpoint with respect to our propositions. Thus, we should calculate the breakpoint probability and it is the same that to calculate the probability to meet a-positive k-series.

At first, let's note that it is natural to consider just those sequences $\{\xi_i\}$ that contain outcome 1 and hence there is at least one k-series inside the sequence.

Secondly, it is notable that if we examine the last k outcomes before the specified time, we receive the ordinary binomial distribution because we explore Bernoulli series. In this connection we have to establish the special proposition.

Proposition 1: *Once the start point of the sequence is specified and it is $\xi_1 = 1$, the k-series cannot be overlap: every new counting of causing events starts just after the previous k-series is over and the next k-series starts from the first outcome 1 detected.*

This proposition should be confirmed by experiment, that is complex enough and at the time we have just one test performed to check it. The result was positive and the proposition was taken into account. We suppose that it holds for the further consideration.

We need to calculate the value of probability of the Markov breakpoint at the specified moment. Suppose that we have just the first N terms in the $\{\xi_i\}$ sequence, i.e., we consider a restricted sequence. Let us denote as

$$\omega = \{(i_1, \epsilon_1), \ldots, (i_m, \epsilon_m)\} \tag{1}$$

an element of the space Ω consists of all possible configurations of k-series within $\{\xi_1, \ldots, \xi_N\}$. Here we have i_l as a start point of k-series number l, ϵ_l as a-positivity indicator of the k-series number l, $l = 1, \ldots, m$, $m \leq [N/k]$ and rectangle braces mean integer part.

Note that $i_{l+1} \geq i_l + k$ and $\epsilon_l \in \{0, 1\}$. There is a set $\hat{\omega}$ of possible instances of the random sequence ξ that corresponds to ω. Now we can proof the next proposition.

Proposition 2: *The following equation*

$$\hat{\omega}^a \cap \hat{\omega}^b = \varnothing$$

holds for any two different ω^a *and* ω^b.

There are following cases correspond to the different ω^a and ω^b:

- $m^a \neq m^b$;
- $m^a = m^b$, but $i_l^a \neq i_l^b$ for at least one l;
- $m^a = m^b$ and $i_l^a = i_l^b$ for all l, but $\epsilon_l^a \neq \epsilon_l^b$ for at least one l.

Otherwise they are coincide.

If $m^a \neq m^b$, let it be $m^a < m^b$. Then there are series with outcome 1 at the position number greater than $i^a_{m^a} + k$ for the set $\hat{\omega}^b$, but none such series in set ω^a.

In case of $m^a = m^b$, but $i_l^a \neq i_l^b$ for at least one l, let's take the minimal l and note that both for ω^a and ω^b the condition $i_l > i_{l-1} + k$ holds ($l > 1$). But we have minimal l taken and hence $i^a_{l-1} = i^b_{l-1}$. This means that sequences from the set $\hat{\omega}^b$ have 0 at the i_l^a position and all sequences from $\hat{\omega}^a$ have 1 there. Hence there is no any intersection.

Finally, when $m^a = m^b$ and $i_l^a = i_l^b$ for all l, but $\epsilon_l^a \neq \epsilon_l^b$ for at least one l, we have the following. All k-series in both $\hat{\omega}^a$ and $\hat{\omega}^b$ sets have common set on start points numbers. In the same time, for some l there are k-series that content different number of 1 for $\hat{\omega}^a$ and $\hat{\omega}^b$ and therefore the sets content no common sequences again. □

From the proven Proposition 2 we derive that there exists probability space $(\Omega, \mathcal{F}, \mathcal{P})$ in Kolmogorov's sense and its elements are determined by (1).

3 Probability in the k-series space

Let us construct a probability measure on the Ω space. Let us define a function $f_l^{a,k}$ determined in Ω in such a way

$$f_l^{a,k} \equiv \begin{cases} 1, & \text{if for } \omega \text{ holds } \sum_{j=1}^{m} \epsilon_j^a = l \\ & 0 \text{ otherwise} \end{cases} \tag{2}$$

A probability to receive l instances of a-positive k-series inside the sequence ξ is equal to

$$P(l, a, k, N, p) = \frac{\sum_{\Omega} f_l^{a,k}(\omega)}{\sum_{l,\Omega} f_l^{a,k}(\omega)}.$$

We need in just values of $P(0, a, k, N, p)$ and $P(1, a, k, N, p)$ for this article purposes.

Let us find the cardinality of the set $\Omega(a, k, N)$. For the fixed m we have

$$M_{mk}^N = C_{N-m(k-1)}^m.$$

We have totally $M = \sum_{m=1}^{\left[\frac{N}{k}\right]} M_{mk}^{N}$ number of elements in the set $\Omega(a,k,N)$ and it is the cardinality of the set.

Probability for the k-series to be a-positive can be easily found from binomial distribution and it has the next form

$$\pi_{ka} = \sum_{i=a}^{k} C_k^i p^i (1-p)^{k-i}. \tag{3}$$

Therefore, the number of cases when the function $f_l^{a,k}$ is equal to 1 for the specified set of $\{1, i_2, \ldots, i_m\}$ can be expressed as follows

$$mC_m^l \left(\pi_{ka}\right)^l \left(1-\pi_{ka}\right)^{m-l}$$

and we can write down the next equality:

$$\sum_{\Omega} f_l^{a,k}(\omega) = \sum_{m=1}^{\left[\frac{N}{k}\right]} C_{N-m(k-1)}^m mC_m^l \left(\pi_{ka}\right)^l \left(1-\pi_{ka}\right)^{m-l}.$$

The explicit expression for the probability on the space Ω of k-series can be presented now. Let us do it in the form of the next proposition.

Proposition 3: *In case if Proposition 1 holds, the probability to have l incidents within first N steps of the sequence $\{\xi_i\}$ has the following form*

$$P(l,a,k,N,p) = \frac{\sum\limits_{m=1}^{\left[\frac{N}{k}\right]} mC_{N-m(k-1)}^m C_m^l \left(\pi_{ka}\right)^l \left(1-\pi_{ka}\right)^{m-l}}{\sum\limits_{m=1}^{\left[\frac{N}{k}\right]} mC_{N-m(k-1)}^m}, \tag{4}$$

where $2 < k < N$, $1 < a < k$ are integer parameters and $0 < p < 1/2$ is real parameter.

4 The Markov breakpoint and measurements

Described above a-positive k-series causes incident. But what if we substantially cannot see it immediately at the end of the k-series? Our decision that we "see" something is based on the information we have got. In order to gather the information there should be done some measurements. Suppose that any measurement that identifies our specified incident takes s steps of the considered sequence $\{\xi_i\}$. Let τ be the measurement duration and hence $\tau = s\nu$, where ν is the duration of a step in the sequence $\{\xi_i\}$. Suppose that any measurement starts immediately after the previous one, i.e., there is no any outcome outside of measurements in the sequence.

Thus, from a practical point of view, one should choose the length N of the sequence that is a multiple of some positive integer s, that shows how many times the sequence step fits inside the measurement duration in the considered system. Therefore we assume

$N = ns$. The first breakpoint can take place at any end of k-series, but just at the end of the s-sequence we can see it and decide that incident occurred.

Let us denote by $F_{a,s,k,p}(n)$ the probability to detect the first incident in nth measurement. If the parameters p, k, a, s have determined values, then the probability $F_{a,s,k,p}(n)$ depends just on the measurement number n and the further outcomes do not affect it value by the definition of the Markov breakpoint. Thus we obviously have

$$F_{a,s,k,p}(n) = P(0, a, k, (n-1)s, p)\,(1 - P(0, a, k, ns, p))\,, \tag{5}$$

where $P(0, a, k, ns, p)$ is determined by the formulas (3) and (4):

$$P(0, a, k, ns, p) = \frac{\sum_{m=1}^{\left[\frac{ns}{k}\right]} mC_{ns-m(k-1)}^{m} \left(\sum\limits_{i=0}^{a-1} C_k^i p^i (1-p)^{k-i}\right)^m}{\sum_{m=1}^{\left[\frac{ns}{k}\right]} mC_{ns-m(k-1)}^{m}}.$$

While we consider some rare incidents, we do not take into account the situation when there are more than one incident detected in the nth measurement.

Having the probability of the first incident to appear at nth measurement, we have information about most dangerous period for the system. Suppose that some asset has assessed risk value R supposed to be constant for a year. However we have received information that an incident similar to those in the threats set of the asset was just detected somewhere. In accordance with our consideration, this fact will affect the probability of the risk anyway. So we should re-evaluate the risk of the asset because it may rise dramatically for a short time and may need to be handled. If $R = P_0 * C$, where P_0 is the risk probability evaluated by common method for a year and C is risk criticality, then the new value of the probability has the next form:

$$P_d = P_0 + 365\frac{1 - P(0, a, k, ds, p\sigma)}{d}, \tag{6}$$

where d shows the duration of increased risk in days and σ is scale factor mentioned before. The value of d can be determined as it is shown further. For the next d days after incident detection it is P_d has to be used for the risk evaluation instead of P_0.

For the real system, the values of the parameters p, k, a, s are unknown, of course. But we can suppose that all these values depend just on the very incident, but not on the system. In this case we can collect statistics on the relevant incidents all over we can. Then it is possible to draw out a posterior probability distribution. The values of p, k, a, s can be determined from this distribution by numerical approximation. Then it is easy to apply them to our target system. This gives us the probability evolution in our system and shows when the probability increases over allowable value.

The distribution of $F_{a,s,k,p}(n)$ for different possible cases are illustrated on the graphs. We consider function (5) on the variable n for different values of parameters a, s, k, p. This function may have a unique local maximum for certain values of the parameters a, s, k, p and this maximum is global if any. The situation is illustrated by graphs in Figures 1–3. They show graphical matrices of probability distributions for different values of parameters.

Figure 1 The probability of the first incident at $p = 0.001$ (see online version for colours)

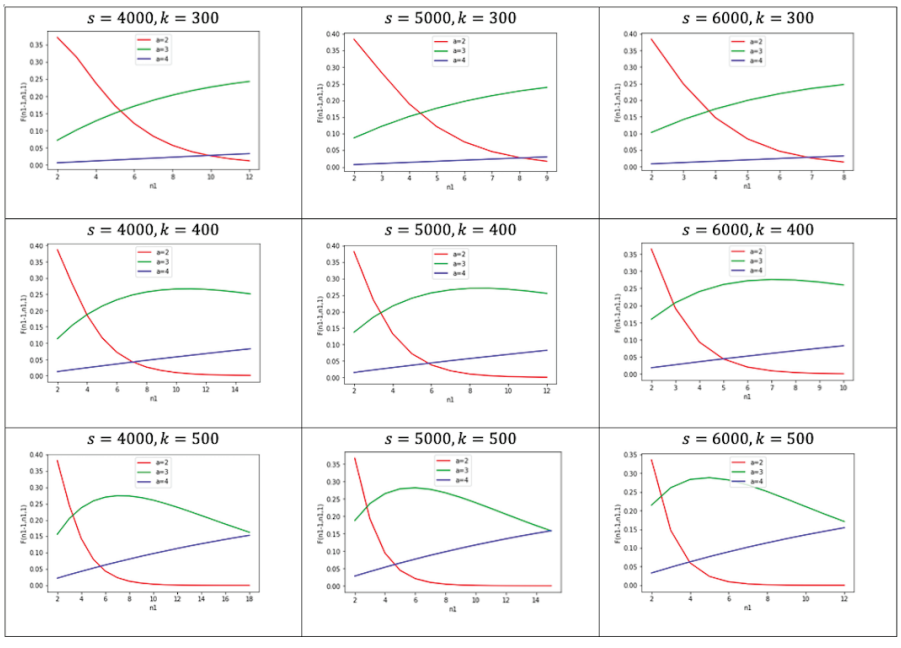
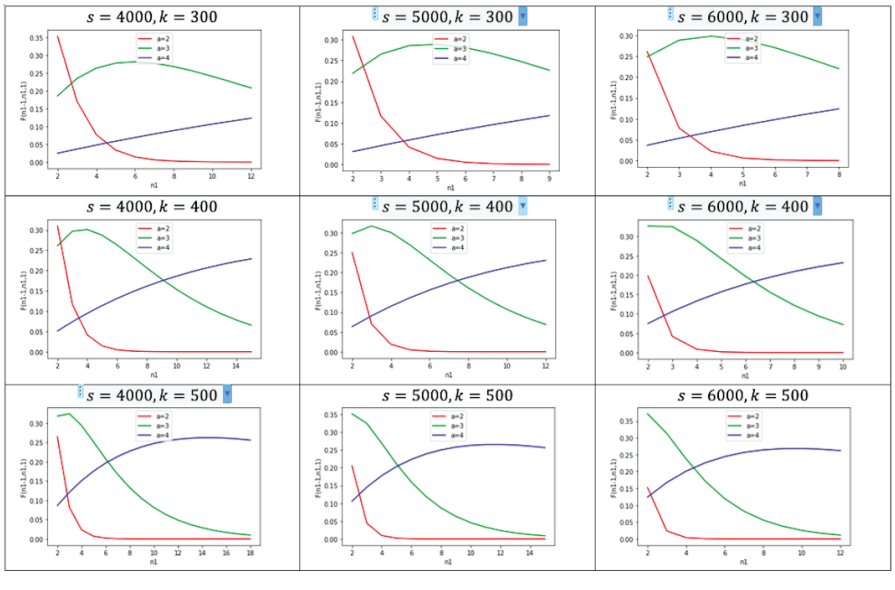


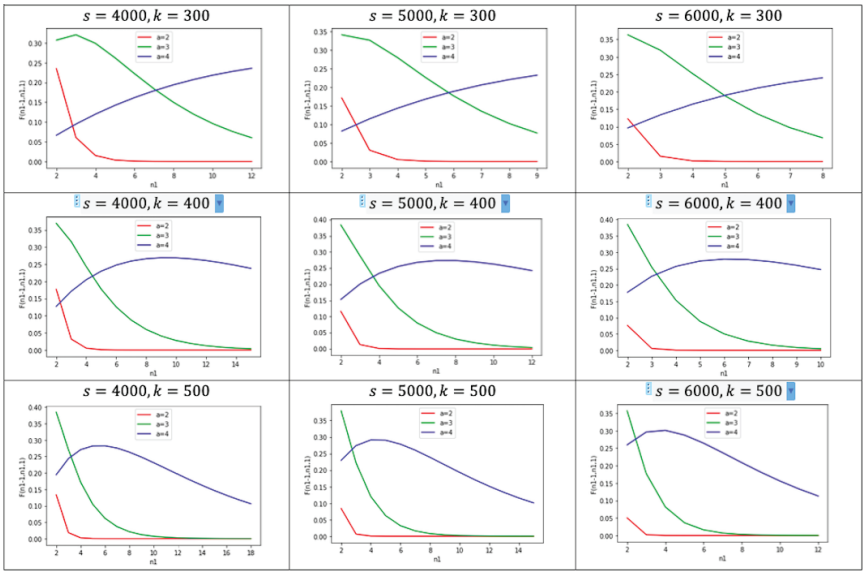
Figure 2 The probability of the first incident at $p = 0.0015$ (see online version for colours)



We see that the maximum exists when the values of k, s or p are great enough. It is connected to the definition of these parameters. The likelihood of the several incidents to be detected within the only measurement is small according to our proposition. It can be easily seen

that the probability depends on the time passed since the last detected incident and almost does not depend on how many incidents were detected before.

Figure 3 The probability of the first incident at $p = 0.002$ (see online version for colours)



5 Results and applications

Suppose we have actual results over the ensemble of the systems for the observations duration equal to, for instance, 365 days. Let us denote as n values of detected durations without incidents in the whole ensemble. For example, there might be 1, 7, 8, 30 and 51 days between neighbour incidents detected during the year and then $n = 1, 7, 8, 30, 51$. We can treat the minimal duration, like a one day in the example, as a measurement duration $s\nu$ and it is some kind of a quant of n. Let g_n be the number of cases when incident occurs after n days since the previous one. Nevertheless we suppose that no more than one incident during one measurement can happen, it was proposition just for the very target system, not for ensemble of the systems. Since we collect the data from the ensemble then we can apply our proposition to any system and hence there are no contradictions. In this case, one can treat equation (5) as the distribution law for g_n. If the parameters a, s, k, p are known, then the probability of an incident at the measurement n is determined by expression (5), where $n = 0$ at the last measurement in the ensemble when an incident detected.

Turn to our target system and now we should evaluate the probability to have the incident there. In order to compute it, we should determine the values of a, s, k, p. It can be done if we suppose that the observed ensemble statistics have the same values of parameters. In this case we have

$$\overline{g} = \frac{\sum\limits_{n} F_{a,s,k,p}(n) g_n}{\sum\limits_{n} F_{a,s,k,p}(n)},$$

where $\overline{g}$ is the theoretical expectation of the most probable first incident frequency. The values of the parameters can be found by minimising the next function

$$\sum_n \left(g_n - \overline{g}(a, s, k, p)\right)^2$$

on the given sample $\{g_n\}$.

Equation (6) can provide us with the new factor P_d in the risk formula and then the new risk value arises

$$R_d = P_d * C$$

It can be much greater than R. The duration d is the only parameter remains unknown in equation (6). We can evaluate it using the form of $F(n)$ function. In the target system there is a defined level R_b of the risk that must be handled with some actions according to the information security policy. In this regard, the inequality

$$R_b < \left(P_0 + 365\frac{1 - P(0, a, k, ds, p\sigma)}{d}\right) C \tag{7}$$

determines the value of d. If there is no such d that obeys inequality, then there is no reason to use new risk value. But if the inequality (7) holds for some d, it is necessary to protect the asset during this period.

To evaluate the value of d for the given parameters, we can use equation (5) as the probability distribution function that determines the breakpoint probability at the nth measurement (day) after the data given. In this case the maximal value of d is equal to the maximal value of n when $F(n)$ is great enough in accordance with risk manager preference. We can then determine not only the duration of the highest probability period, but the most probable next breakpoint time as well. The periods of high probability can be easily recognised on the graphs and, of course, can be automatically computed once the actual data given.

For example, suppose that $\sigma = 0.01$, i.e., 100 systems similar to the target system are observed. Let observations and approximation give us values of $a = 3$, $s = 5000$, $k = 400$ for $p = 0.001$. In this regard, the central green graph on the Figure 1 is relevant to the case. Let the risk manager decides that first 12 days are dangerous, hence $d = 12$. Let the criticality and the base risk are $C = 10^8$ and $R_0 = 100$ whereas $R_b = 2000$. Then we can compute $1 - P(0, a, k, ds, p\sigma) = 1.3 * 10^{-6}$ and

$$P_d = \frac{R_0}{C} + 365\frac{1 - P(0, a, k, ds, p\sigma)}{d} = 4 * 10^{-5}.$$

After that we have $R_d = 4000$ during those 12 days and the risk must be handled.

6 Conclusion

This study was initiated as a part of a research project in information security field. The risks considered in the project are assessed according to the video data. However, the result

of the paper is of general type and it can be used both in the cybersecurity and reliability theory risk management.

The proposed model describes the rare incidents and can be applied to dynamical risk evaluation; this model may be the first one of such type. The most useful application of the model may be for artificial random threats in information security. These threats are associated with around of 2/3 of all damages associated with information security incidents. The relevant risks to these threats are difficult to be managed and arranged. The proposed model quantitatively estimates probability part of the risks and it is enough to compute the risk value because the criticality of the assets is assessed by experts. The model can help to manage risks of “black swan” type as well. Note that the "black swans" are commonly among accepted risks and it is not because of its lowness, but rather because of the absence of common ways to manage them. It is possible to apply the ideas and technique proposed in the paper to predict further incidents at the specified time and, thereby, build an automated system for assessing information security risks.

Acknowledgement

The project is funded in part by the Russian Foundation for Basic Research, under Project No. 19-29-09056.

Both authors have common research project for 2019–2022.

References

Astahov, A.M. (2010) *Art of Information Risk Management*, DMK Press, Moscow.

Gnedenko, B.V., Belyayev, Yu.K. and Solovyev, A.D. (1969) *Mathematical Methods of Reliability Theory*, trans. by Scripta Technica, trans. ed. by Richard E. Barlow, NY, Academic Press.

Havinga, H.N.J. and Sessink O.D.T. (2014) ‘Risk reduction overview’, in Teufel, S., Min, T.A., You, I. and Weippl, E. (Eds.): *Availability, Reliability, and Security in Information Systems. CD-ARES 2014*, Lecture Notes in Computer Science, Vol. 8708, Springer, Cham, pp.239–249.

Karbowski, A., Malinowski, K., Szwaczyk, S. and Jaskóla, P. (2019) ‘Critical infrastructure risk assessment using Markov chain model’, *Journal of Telecommunications and Information Technology*, Vol. 2, pp.15–20.

McCarthy (2020) *The Ergodic Theorem for Random Walks on Finite Quantum Groups*, [Online] Available at: https://arxiv.org/abs/2004.01234 (Accessed 2 April, 2020).

Shiryaev, A.N. (1978) *Optimal Stopping Rules*, 2nd English ed., Springer-Verlag, New York.

Shiryaev, A.N. (1996) *Probability*, Grad. Texts in Math., Vol. 95, SpringerVerlag, New York.

Taleb, N.N. (2007) *The Black Swan: The Impact of the Highly Improbable*, Random House and Penguin Books, New York.

van Handel R. (2014) ‘Ergodicity, decisions, and partial information’, in Donati-Martin, C., Lejay, A. and Rouault, A. (Eds.): *Séminaire de Probabilités XLVI. Lecture Notes in Mathematics*, Vol. 2123, Springer, Cham, pp.411–459.