ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.05653
DOI: 10.21822/2073-6185-2022-49-3-39-51 Оригинальная статья /Original Paper

Об оценке устойчивости функционирования объекта информатизации в условиях компьютерных атак при экспоненциальном законе распределения времени до воздействия противника и восстановления работоспособности

В.А. Воеводин, И.В. Виноградов, Д.И. Волков
Национальный исследовательский университет
«Московский институт электронной техники»,
124498, г. Москва, г. Зеленоград, пл. Шокина, 1, Россия

Резюме. Цель. Целью исследования является разработка математической модели оценки устойчивости функционирования объекта информатизации (ОИ) в условиях компьютерных атак (КА) при принятии ограничения о том, что случайные величины времени до воздействия противника и времени восстановления работоспособности распределены по экспоненциальному закону. **Метод.** Приложение метода дискретных марковских процессов для решения задачи по оценке устойчивости ОИ, отличающегося от известных подходов тем, что для описания состояния ОИ вводится понятие «невозвратное состояние», в которое система может переходить из-за исчерпания ресурса, выделенного для восстановления его готовности после успешной КА. **Результат.** В результате исследования разработана математическая модель, позволяющая строить функцию устойчивости ОИ с учетом интенсивности потока КА и интенсивности восстановления его работоспособности при учете ограничения на выделенный ресурс. **Вывод.** Применение метода позволяет осуществлять количественную оценку устойчивости функционирования ОИ посредством построения функции живучести ОИ в условиях КА, при которых потоки атак и восстановлений нельзя принять стационарными и эргодическими, а также отсутствует репрезентативная статистика для расчета асимптотических оценок устойчивости. Количественная оценка устойчивости ОИ в условиях КА востребована органами управления информационной безопасностью при принятии решения по обеспечению защиты информации, а также при обосновании требований к системе восстановления работоспособности.

Ключевые слова: объект информатизации, устойчивость функционирования объекта информатизации, компьютерная атака, массированная компьютерная атака, готовность объекта информатизации, частные и агрегированный показатели устойчивости, аудит информационной безопасности

Для цитирования: В.А.Воеводин, И.В.Виноградов, Д.И.Волков. Об оценке устойчивости функционирования объекта информатизации в условиях компьютерных атак при экспоненциальном законе распределения времени до воздействия противника и восстановления работоспособности. Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(3): 39-51. DOI:10.21822/2073-6185-2022-49-3-39-51

About the informatization object functioning stability assessment in conditions of computer attacks at exponential distribution law of time before the enemy’s impact

V.A. Voevodin, I.V. Vinogradov, D.I. Volkov
National Research University of Electronic Technology,
1 Shokina Square, Moscow, Zelenograd 124498, Russia

Abstract. Objective. The aim of the study is to develop a mathematical model for assessing the stability of the functioning of an informatization object (IO) in the conditions of computer attacks (CA), assuming that the laws of distribution of random variables before the enemy's impact and the recovery time are distributed exponentially. **Method.** Application of the method of discrete Markov processes to solve the problem of assessing the stability of IO, which differs from the known approaches in that to describe the state of IO, the concept of "non-returnable state" is introduced, into which the system can move due to the exhaustion of the resource allocated to restore its readiness after a successful CA. **Result**. As a result of the research, a mathematical model has been developed that allows us to build the stability function of the IO taking into account the intensity of the CA flow and

the intensity of restoring its operability, taking into account the limitations on the allocated resource. **Conclusion.** The application of the method makes it possible to quantify the stability of the functioning of the IO by constructing the survivability function of the IO for conditions under which the flows of attacks and recoveries cannot be assumed stationary and ergodic, and there is also no representative statistics for calculating asymptotic estimates of stability. A quantitative assessment of the stability of the IO for the conditions of the CA is in demand by information security management bodies when making decisions to ensure the protection of information, as well as when justifying the requirements for the system to restore operability.

Keywords: informatization object, stability of functioning of informatization object, computer attack, massive computer attack, readiness of informatization object, private and aggregated stability indicators, information security audit

For citation: V.A. Voevodin, I.V. Vinogradov, D.I. Volkov. About the informatization object functioning stability assessment in conditions of computer attacks at exponential distribution law of time before the enemy's impact. Herald of the Daghestan State Technical University. Technical Science. 2022; 49 (3): 39-51. DOI: 10.21822 /2073-6185-2022-49-3-39-51

Введение. Сведения о динамике среды киберпреступлений приведены в [1, 2]. В силу закона [3] обладатель информации, сообразуясь с развитием среды киберпреступлений, обязан принимать меры по защите информации (ЗИ) и недопущению воздействия на технические средства обработки информации, в результате которого нарушается их процесс функционирования объекта информатизации (ОИ).

Под объектом информатизации могут рассматриваться и отдельные элементы, входящие в состав ОИ, которые могут быть объединены в соответствующую систему для исследования устойчивости функционирования системы в целом. Для принятия результативного решения по защите ОИ в условиях компьютерных атак (КА) требуются исходные данные об обстановке, в том числе и об устойчивости функционирования самого объекта защиты, в роли которого выступает сам ОИ или его отдельные подсистемы. Оценка устойчивости ОИ, предназначенного для применения в условиях КА, может быть востребована: органами управления информационной безопасностью (ИБ) при задании требований к устойчивости функционирования отдельных элементов ОИ и ОИ в целом [4, 5]; лицами, управляющими программами аудита ИБ, при формировании критериев аудита, а также при разработке программ и методик аудиторских испытаний [6, 7]; лицами, проводящими оценку рисков информационной безопасности (ИБ) с целью обоснования страховых тарифов [8]; лицами, управляющими рисками ИБ [9] и др.

Исходные данные, необходимые для принятия решения по ЗИ, добываются в результате аудита информационной безопасности. Общие вопросы организации и проведения аудита систем управления информационной безопасностью для штатных условий рассмотрены в национальных стандартах [6, 7], а также в работах [10 - 13]. Однако вопросы оценки устойчивости объекта в условиях КА исследованы недостаточно полно, что не позволяет сформировать научно обоснованные рекомендации по её аудиторской оценке.

Обозначенный предмет исследования представляет практический и теоретический интересы, поскольку методы, разрабатываемые теорией надежности, ориентированы на простые, стационарные и эргодические потоки отказов, что нельзя применить к условиям аномальных воздействий, в том числе и к условиям КА [14]. В условиях КА период работоспособного состояния объекта соизмерим со временем его восстановления, поэтому применение модели пуассоновского потока отказов для оценки устойчивости ОИ приводит к существенным погрешностям. Более того, принципиально отсутствуют условия для сбора репрезентативной статистики, что не позволяет получить достоверные асимптотические оценки устойчивости ОИ в условиях КА. В целях обеспечения достоверности результатов моделирования требуется применение модели альтернирующего процесса, где время восстановления соизмеримо с периодом функционирования объекта и имеет конечную величину, при этом аналитические модели реального процесса функционирования громоздки, трудно интерпретируемы и не нашли практического применения [14].

Стационарный процесс функционирования ОИ в условиях старения его элементов и штатной эксплуатации может прерываться аномальными воздействиями внешней среды, в том числе и целенаправленными, приводящими к его повреждению. К таким воздействиям могут относиться стихийные бедствия, одиночные или массированные КА, которые имеют следующие особенности: значительные повреждения ОИ, приводящие к существенному увеличению

времени восстановления; незначительное время между соседними повторными КА; ограниченное число целенаправленных КА на относительно небольшом промежутке времени; отличие законов распределения случайных величин времени до повреждения и времени восстановления работоспособности от аналогичных законов при штатной эксплуатации; вид и параметры законов распределения на практике чаще неизвестны из-за отсутствия репрезентативной статистики по причине редкости названных событий.

С учетом этих особенностей применение классического подхода, приведенного в [15, 16] для оценки устойчивости исследуемого ОИ и её асимптотических оценок, может привести к существенным ошибкам при принятии решения по обеспечению ИБ в условиях аномальных и целенаправленных воздействий внешней среды.

Постановка задачи. А) Определены исходные данные:

- атрибуты интенсивности КА, $\lambda = \{\mathbb{F}(t), n\}$, включающие множество функций распределения $\mathbb{F}(t)$ случайных интервалов времени η_i, до очередной i-й КА, $\mathbb{F}(t) = \{F_i(t)\}$, где $F_i(t)$ – функция распределения случайного η_i интервала времени до i-ой КА, i = 1, 2, …, n, n – число атак в составе КА;
- характеристики $u = \{T_н, \mathbb{P}\}$ надежности и живучести ОИ, включающие наработку между отказами ОИ $T_н$ в нормальных условиях применения и множество вероятностей поражения ОИ в результате КА, $\mathbb{P} = \{P_i\}$, где P_i – вероятность поражения ОИ при i-й КА. Подход к определению вероятностей поражения с применением экспертных методов приведён в [17, 18, 19];
- r - варьируемые (изменяемые) характеристики восстанавливаемости ОИ, $r = \{T_в, \mathbb{G}(t)\}$, где $T_в = \{\tau^н_{вi}, \tau^в_{вi}\}$ – прогнозируемый интервал времени восстановления (временная избыточность) после i-й КА; $\mathbb{G}(t)$ – множество функций распределения случайных интервалов времени восстановления работоспособности (временной избыточности) после i-й КА, $\mathbb{G}(t) = \{G_i(t)\}$. Порядок экспертной оценки нижней $\tau^н_{вi}$ и верхней $\tau^в_{вi}$ границ случайной величины времени восстановления ОИ $T_в = \{\tau^н_{вi}, \tau^в_{вi}\}$ после i-й КА приведен в [17];
- требуемый для восстановления работоспособности ОИ после успешной КА ресурс $R_0 = \{T_0, r_0\}$, где T_0 – допустимое (требуемое) время восстановления работоспособности ОИ, r_0 – требуемый ресурс сил и средств для восстановления работоспособности ОИ;
- выделенный для восстановления работоспособности ОИ ресурс $R = \{T, r\}$, где T – назначенное время для восстановления работоспособности ОИ, r – выделенный ресурс для восстановления работоспособности ОИ.

Б) Требуется разработать аналитическую процедуру и исследовать частные случаи определения наименьшего значения ν_m функции устойчивости ОИ на заданном интервале (0, T]):

$$\nu_m = \inf_{\substack{t \in (0,\,T],\\ R \le R_0}} \nu(t, \lambda, r, u).$$

Функция устойчивости ОИ в общем виде записывается как [14]:

$$\nu(t, \lambda, r, u) = K_Г(u, r)\varphi(t, \lambda, r, u),$$

где $K_Г(u, r)$ – коэффициент готовности ОИ; $\varphi(t, \lambda, r, u)$ – функция живучести (ФЖ) ОИ; t – текущий момент времени оценки ФЖ; T – интервал времени ожидания КА.

Общий порядок определения коэффициента готовности ОИ приведен и исследуется в теории надежности технических систем [20]: $K_г = T_н(T_н + T_в)^{-1}$,

где $T_н$ – среднее время наработки на отказ в штатных условиях эксплуатации, $T_в$ – среднее время восстановления работоспособности в штатных условиях эксплуатации – определяются на основании статистических наблюдений, полученных в условиях штатной эксплуатации ОИ.

Для большинства случаев $K_Г \ge 0{,}99$, а наименьшее значение ФЖ $\varphi_m << K_Г$, поэтому $K_Г$ при оценке живучести можно пренебречь. Тогда математическая модель сводится к определению $\nu_m \approx \varphi_m = \inf\ \varphi(t, \lambda, r, u)$, где ν_m – минимальное значение функции устойчивости на задан-

ном интервале времени, φ_m – минимальное значение функции живучести на периоде нанесения КА по ОИ.

Задача решается в два этапа:

1) определение вида оператора A: $\varphi(t) = A\{\mathbb{F}(t), \mathbb{G}(t), \mathbb{P}, n\}$; 2) определение функционала $\varphi_m = \inf_{t \in (0, t]} \varphi(t)$.

Наиболее сложным является первый этап, в ходе которого рассматриваются различные виды оператора A и осуществляется выбор приемлемого:

- оператор A_0, определяемый при произвольных законах распределения $F_i(t)$ и $G_i(t)$ и различных P_i (общий полумарковский процесс восстановления). В этом случае процесс восстановления можно характеризовать как общий полумарковский. Это тема последующей – третьей публикации;
- оператор A_1, определяемый при одинаковых законах распределения $F_i(t) = F(t)$ и $G_i(t) = G(t)$ и равных $P_i = P$. В этом случае процесс восстановления можно позиционировать как частный полумарковский. Это тема последующей - второй публикации;
- оператор A_2, определяемый при экспоненциальных законах распределения времени до КА F(t) и времени восстановления работоспособности ОИ G(t), таких, что $F(t) = 1 - e^{-\lambda t}$, $G(t) = 1 - e^{-\mu t}$, где λ и μ – параметры экспоненциального распределения времени до КА и времени восстановления работоспособности ОИ соответственно; $P_i = P$, как в A_1.

В этом случае процесс можно характеризовать как дискретный марковский – это тема настоящего исследования и публикации.

Методы исследования. Описание дискретного марковского процесса. Дискретный марковский процесс характеризуется тем, что время t, на котором определяются возможные состояния ОИ, непрерывно, а случайные состояния ОИ z(t) в сечении t принимают конечные или счетные значения из множества Z. Множество Z содержит конечное число n состояний. Ограничение вводится с помощью математической модели:

$$z(t) \in Z,\ Z = \{z_i,\ i = 1, 2, \ldots, n\}.$$

В соответствии с этим вместо вероятных i-х состояний ОИ z_i при математическом моделировании можно рассматривать только индексы этих состояний. Для моделирования смены состояний ОИ в качестве исходного можно использовать множество мощностью m^2 условных интервально-переходных вероятностей:

$$P_{ij}(t_0, t),\ i, j = 1, 2, \ldots, m,$$

При этом принимается, что вероятностная модель удовлетворяют следующим условиям:

1. Сумма вероятностей по всем возможным состояниям в момент t равна единице:
$$\sum_{j=1}^{m} P_{ij}(t_0, t) = 1;$$
2. При $t_0 = t$ вероятность равна единице, когда i = j, в остальных случаях равна нулю, т. е. описывается символом Кронекера:
$$\forall t_0, t:\ t_0 = t\ P_{ij}(t_0, t) = \delta_{ij} = \begin{cases} 1 \text{ при } i = j; \\ 0 \text{ при } i \neq j; \end{cases}$$
3. Вероятности удовлетворяют уравнениям Колмогорова-Чепмена для любого промежуточного момента времени t': $t_0 < t' < t$:
$$P_{ij}(t_0, t) = \sum_{k=1}^{m} P_{ik}(t_0, t')P_{kj}(t', t),\ i, j = 1, 2, ..., m. \qquad (1)$$

Уравнения (1) позволяют определить вероятности состояний двух крайних сечений в моменты t_0 и t по известным условным интервально-переходным вероятностям относительно промежуточного сечения в момент t':

$$P(i, t_0, j, t) = P_j(t_0)P_{ij}(t_0, t'),\ \ i, j = 1, 2, ..., m,$$

где $P_j(t_0)$ – вероятность состояния z_j в момент t_0.

Если известны начальные вероятности i-х состояний в момент t_0 и найдены $P_{ij}(t_0, t)$, то можно определить вероятность любого j-го состояния в момент t по формуле

$$P_j(t) = \sum_{i=1}^{m} P_i(t_0)P_{ij}(t_0, t),\ \ i, j = 1, 2, \ldots, m.$$

Вероятности $P_{ij}(t_0, t)$ определяются путем решения следующей системы дифференциальных уравнений:

$$P'_{ij}(t_0, t) = \sum_{k=1,\, k\neq j}^{m} \left[\lambda_{kj}(t)P_{ik}(t_0, t) - \lambda_{jk}(t)P_{ij}(t_0, t)\right],\ \ i, j = 1, 2, \ldots, m, \qquad (2)$$

где $\lambda_{kj}(t), \lambda_{jk}(t)$ – интенсивности переходов из состояний k в j или j в k, определяющие частоту соответствующих переходов в единицу времени:

$$\lambda_{kj} = \lim_{\Delta t \to 0} \frac{P_{kj}(t_0, t)}{\Delta t};\ \lambda_{jk}(t) = \lim_{\Delta t \to 0} \frac{P_{jk}(t_0, t)}{\Delta t}.$$

Система уравнений (2) выводится путем преобразования уравнения (1) и позиционируется как система обратных уравнений Колмогорова.

Аналогично может быть получен вывод дифференциальных уравнений для безусловных вероятностей $P'_j(t)$ j-х состояний процесса в любой момент времени:

$$P'_j(t) = \sum_{k=1,\, k\neq j}^{m} \left[\lambda_{kj}(t)P_k(t) - \lambda_{jk}(t)P_j(t)\right],\ \ j = 1, 2, \ldots, m. \qquad (3)$$

Система (3) позиционируется как система прямых уравнений Колмогорова.

Решение (2) и (3) для реальных случаев сопряжено со значительными трудностями вычислительного характера, поэтому целесообразно ввести ряд допущений.

Во-первых, принимается, что исследуемый марковский процесс является однородным. Для однородного процесса можно принять, что вероятности $P_{ij}(t_0, t)$ будут зависеть только от разности $\tau = t - t_0$, т. е. $P_{ij}(t_0, t) = P_{ij}(\tau)$, а интенсивности $\lambda_{ij}(t)$ будут постоянными величинами $\lambda_{ij}(t) = \lambda_{ij}$, причем: $P_{ij}(\tau) = \pi_{ij}F_{ij}(\tau) = \pi_{ij}F_i(\tau)$, $\lambda_{ij} = \pi_{ij}\lambda_i$,

где $F_i(\tau) = 1 - e^{-\lambda_i\tau}$ – функция распределения времени пребывания ОИ в состоянии z_i, а π_{ij} – постоянные интенсивности переходов ОИ из состояния z_i в z_j.

В результате дифференциальные уравнения (3) принимают следующий вид:

$$P'_j(t) = \sum_{k=1,\, k\neq j}^{m} \left[\lambda_{kj}P_k(t) - \lambda_{jk}P_j(t)\right],\ \ j = 1, 2, \ldots, m. \qquad (4)$$

Во-вторых, принимается, что однородный марковский процесс обладает эргодическими свойствами и существует однозначно-определенное (равновесное) состояние при $t \to \infty$. В этом случае существуют предельно-постоянные значения вероятностей $P_j(t)$:

$$\lim_{t \to \infty} P_j(t) = P_j.$$

В итоге дифференциальные уравнения (4) преобразуются в систему линейных алгебраических уравнений относительно P_j:

$$0 = \sum_{k=1,\, k\neq j}^{m} \left[\lambda_{kj}P_k - \lambda_{jk}P_j\right],\ \ j = 1, 2, \ldots, m. \qquad (5)$$

В-третьих, ограничивается число допустимых переходов из состояний k в j и j в k, что позволяет сократить число слагаемых в уравнениях (5). Например, для процесса «размножения

и гибели» предполагается, что переходы возможны только в соседние состояния. Тогда уравнения (5) принимают следующий вид:

$$\lambda_{j-1}P_{j-1} + (\lambda_{j-} + \mu_j)P_j + \mu_{j+1}P_{j+1},\ j = 1, 2, \ldots, m, \tag{6}$$

где $\lambda_{j-1} = \lambda_{j-1, j}$; $\lambda_{j+1} = \lambda_{j, j+1}$ – интенсивности переходов (повреждений) из состояний j в (j + 1) соответственно; $\mu_j = \lambda_{j, (j-1)}$; $\mu_{j+1} = \lambda_{(j+1), j}$ – интенсивности переходов (восстановлений работоспособности) из состояний j и (j + 1) в состояния (j – 1) и j соответственно; $\lambda_0 = \mu_1 = \lambda_n = \mu_{n+1} = 0$, т. к. $0 < j \le m$, где $\lambda_0 = \lambda_{j-1}$.

Решение систем уравнений (4), (5), (6) осуществляется при соблюдении нормирующего условия:

$$\sum_{j=1}^{m} P_j = 1.$$

Определение функции живучести. Заданы КА – n и вероятность поражения ОИ – P < 1 при каждом воздействии. Граф переходов подобного ДМП представлен на рис.1.

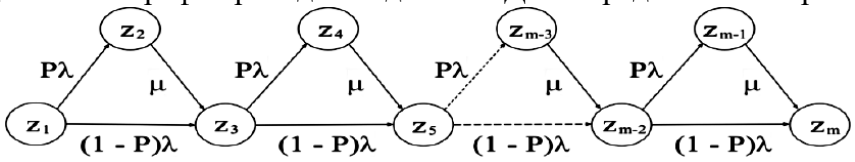

Рис.1. Граф переходов дискретного марковского процесса
Fig.1. Transition graph of a discrete Markov process

Число m, индексы i состояний z_i процесса и вероятности переходов совпадают с соответствующими характеристиками полумарковского процесса, однако исследуемый ДМП имеет следующие особенности:

1. Процесс является однородным и характеризуется постоянными интенсивностями λ_{ik} переходов из состояния z_i в z_k; i, k = 1, 2, …, m, причем $\lambda_{ik} = \pi_{ik}\lambda_i$, где λ_i – параметр экспоненциального закона распределения времени пребывания процесса в состоянии z_i;
2. Случайное время пребывания процесса в состояниях с нечетными индексами i = 2j + 1 распределено по закону $F_{2j+1}(t) = 1 - e^{-\lambda t}$, j = 1, 2, …, (n – 1); и четными i = 2j – по закону $F_{2j}(t) = 1 - e^{-\mu t}$, j = 1, 2, …, n.
3. Интенсивности переходов процесса из состояния z_i в z_k имеют следующие ния: $\lambda_{ik} = 0$ при $i \ge k$, k – i > 2; $\lambda_{2j, (2j+1)} = \mu$; $\lambda_{(2j-1), 2j} = P\lambda$;

$\lambda_{(2j-1), (2j+1)} = (1 - P)\lambda$, j = 1, 2, …, n.

С учетом данных особенностей система дифференциальных уравнений (4) примет следующий вид:

$$\begin{gathered}
P'_1(t) = -\lambda P_1(t); \\
\ldots\ldots\ldots\ldots\ldots \\
P'_i(t) = -\mu P_i(t) + P\lambda P_{i-1}(t);\ i = 2j,\ j = 1, 2, \ldots, n; \\
P'_i(t) = -\lambda P_i(t) + \mu P_{i-1}(t) + (1 - P)\lambda P_{i-2}(t);\ i = 2j + 1,\ j = 1, 2, \ldots, (n - 1); \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
P'_m(t) = \mu P_{m-1}(t) + (1 - P)\lambda P_{m-2}(t);\ m = 2n + 1; \\
\sum_{j=1}^{m} P_j(t) = 1.
\end{gathered} \tag{7}$$

Искомая ФЖ φ(t) будет равна сумме безусловных вероятностей состояний z_i, соответствующих исправному ОИ, т. е. состояний, индексы которых i = 2j + 1. В результате

$$\varphi(t) = \sum_{j=1}^{m} P_{2j+1}(t). \tag{8}$$

Для нахождения ФЖ к системе (7) и уравнению (8) применяется преобразование Лапласа с учетом следующих начальных условий: $P_1(0) = 1$, $P_i(0) = 0$, $i \neq 1$.

При определении начальных условий принимается, что в начальный момент времени $t_0 = 0$ ОИ всегда находится в исправном состоянии, т. е. $z_1 = 1$.

В результате получается следующая система уравнений:

$$\begin{gathered}
s\widetilde{P_1}(s) - 1 = -\lambda\widetilde{P_1}(s); \\
\ldots\ldots\ldots\ldots\ldots\ldots \\
s\widetilde{P_i}(s) = -\mu\widetilde{P_i}(s) + P\lambda\widetilde{P_{i-1}}(s);\ i = 2j;\ j = 1, 2, \ldots, n; \\
s\widetilde{P_i}(s) = -\lambda\widetilde{P_i}(s) + \mu\widetilde{P_{i-1}}(s) + (1-P)\lambda\widetilde{P_{i-2}}(s);\ i = 2j+1;\ j = 1, 2, \ldots, (n-1); \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
s\widetilde{P_m}(s) = \mu\widetilde{P_{m-1}}(s) + (1-P)\lambda\widetilde{P_{m-2}}(s);\ m = 2n+1;
\end{gathered} \tag{9}$$

$$\sum_{j=1}^{m} \widetilde{P_j}(s) = s^{-1}, \tag{10}$$

где s – аргумент изображения ФЖ.

Преобразование Лапласа $\varphi(t)$ будет иметь вид

$$\widetilde{\varphi}(s) = \sum_{j=1}^{m} \widetilde{P_{2j+1}}(s). \tag{11}$$

Произведем суммирование левой и правой частей уравнений (9), содержащих $\widetilde{P_i}(s)$ с нечетными индексами $i = 2j + 1$; $j = 0, 1, \ldots, (n-1)$, и с учетом (10) и (11) получаем:

$$s\widetilde{\varphi}(s) - 1 = -\lambda\left[\widetilde{\varphi}(s) - \widetilde{P_m}(s)\right] + \mu[s^{-1} - \widetilde{\varphi}(s)] + (1-P)\lambda\left[\widetilde{\varphi}(s) - \widetilde{P_m}(s)\right],$$

$$\widetilde{\varphi}(s) = s^{-1} - \lambda P\left[1 - s\widetilde{P_m}(s)\right][s(s + \lambda P + \mu)]^{-1}. \tag{12}$$

Выражение для $\widetilde{P_m}(s)$ находим, решая систему уравнений (9) методом подстановки, и получаем:

$$\widetilde{P_m}(s) = [\mu\lambda + (1-P)\lambda s]^n[s(s+\lambda)^n(s+\mu)^n]^{-1}. \tag{13}$$

Подставляя (13) в (12), получаем выражение для преобразования Лапласа ФЖ:

$$\widetilde{\varphi}(s) = \frac{\lambda P\{[(s+\mu)(s+\lambda)]^n - [\mu\lambda + (1-P)\lambda s]^n\}}{s(s + \lambda P + \mu)[(s+\mu)(s+\lambda)]^n}.$$

Полученное выражение представляется в виде, удобном для применения обратного преобразования Лапласа:

$$\widetilde{\varphi}(s) = s^{-1} + \lambda P \sum_{i=1}^{n} \lambda^{i-1}\widetilde{\alpha}_i(s),$$

$$\text{где } \widetilde{\alpha}_i(s) = \frac{(s + \mu - Ps)^{i-1}}{(s+\lambda)^i(s+\mu)^i} = \sum_{j=0}^{i-1}\left[\frac{D_{i-j}}{(s+\lambda)^{i-j}} + \frac{B_{i-j}}{(s+\mu)^{i-j}}\right]. \tag{14}$$

Значения D_{i-j} и B_{i-j} определяются с использованием методов разложения отношения $g(s)/f(s)$ многочлена $g(s)$ степени m и многочлена $f(s)$ степени n такой, что $n > m$, на сумму элементарных дробей. Для рассматриваемого случая получаем:

$$g(s) = (s + \mu - Ps)^{i-1},\ f(s) = (s+\lambda)^i(s+\mu)^i,\ m = i - 1,\ n = 2i,$$

причем многочлен $f(s)$ имеет два корня $-\lambda$ и $-\mu$ кратности i. Наиболее приемлемым является метод поиска искомых коэффициентов в условиях рассматриваемой задачи, основанный на последовательном дифференцировании равенства

$$g(s) = f(s)\sum_{j=0}^{i-1}\left[\frac{D_{i-j}}{(s+\lambda)^{i-j}}+\frac{B_{i-j}}{(s+\mu)^{i-j}}\right]$$

с подстановкой значений $s = -\lambda$ или $s = -\mu$.

В результате коэффициенты $D_i, D_{i-1}, ..., D_1$ и $B_i, B_{i-1}, ..., B_1$ последовательно находятся из соотношений

$$\begin{gathered}(\mu-\lambda+P\lambda)^{i-1}=(\mu-\lambda)^{i}D_i;\\ (i-1)(1-P)(\mu-\lambda+P\lambda)^{i-2} = i(\mu-\lambda)^{i-1}D_i + (\mu-\lambda)^{i}D_{i-1};\\ (i-1)(i-2)(1-P)^2(\mu-\lambda+P\lambda)^{i-3} = i(i-1)(\mu-\lambda)^{i-2}D_i +\\ + 2i(\mu-\lambda)^{i-1}D_{i-1} + 2(\mu-\lambda)^{i}D_{i-2};\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ (i-1)!(1-P)^{i-1} = i(i-1)\ldots 2(\mu-\lambda)D_i + i^2(i-1)\ldots 3(\mu-\lambda)^2D_{i-1} + \ldots + i!D_i;\end{gathered} \tag{15}$$

$$\begin{gathered}(P\mu)^{i-1}=(\mu-\lambda)^{i}B_i;\\ (i-1)(1-P)(P\mu)^{i-2} = i(\mu-\lambda)^{i-1}B_i + (\mu-\lambda)^{i}B_{i-1};\\ (i-1)(i-2)(1-P)^2(P\mu)^{i-3} = i(i-1)(\mu-\lambda)^{i-2}B_i +\\ + 2i(\mu-\lambda)^{i-1}B_{i-1} + 2(\mu-\lambda)^{i}B_{i-2};\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ (i-1)!(1-P)^{i-1} = i(i-1)\ldots 2(\mu-\lambda)B_i + i^2(i-1)\ldots 3(\mu-\lambda)^2B_{i-1} + \ldots + i!B_i;\end{gathered} \tag{16}$$

Общие аналитические выражения для коэффициентов D_{i-j} и B_{i-j}, полученные из соотношений (15) и (16), являются достаточно громоздкими. При $P = 1$ поиск решения несколько упрощается и сводится к преобразованию следующих изображений ФЖ:

$$\tilde{\varphi}(s) = s^{-1} + \lambda\sum_{i=1}^{n}(\lambda\mu)^{i-1}\tilde{\beta}_i(s), \tag{17}$$

$$\text{где } \tilde{\beta}_i(s) = \frac{1}{(s+\lambda)^i(s+\mu)^i} = \sum_{j=0}^{i-1}\left[\frac{D_{i-j}}{(s+\lambda)^{i-j}} + \frac{B_{i-j}}{(s+\mu)^{i-j}}\right], \tag{18}$$

$$D_{i-j} = (-1)^i C_{i+j-1}^{i-1}(\mu-\lambda)^{-(i+j)},\ B_{i-j} = (-1)^j C_{i+j-1}^{i-1}(\lambda-\mu)^{-(i+j)},$$

C_x^y – число сочетаний из x элементов по y; $x, y \in \mathbb{N}$.

Для обращения полученных преобразований Лапласа (14), (18) используем соответствия между изображениями и оригиналами формулы:

$$\frac{D_{i-j}}{(s+\lambda)^{i-j}} \to \frac{D_{i-j}}{(i-j-1)!}t^{i-j-1}e^{-\lambda t},\ \frac{B_{i-j}}{(s+\mu)^{i-j}} \to \frac{B_{i-j}}{(i-j-1)!}t^{i-j-1}e^{-\mu t}.$$

В результате получаем следующие итоговые выражения:

$$\varphi(t) = 1 - \lambda P\sum_{i=1}^{n}\lambda^{i-1}\alpha_i(t), \tag{19}$$

$$\text{где } \alpha_i(t) = \sum_{j=0}^{i-1}\frac{t^{i-j-1}}{(i-j-1)!}(D_{i-j}e^{-\lambda t} + B_{i-j}e^{-\mu t}), \tag{20}$$

D_{i-j} и B_{i-j} определяются с помощью соотношений (15) и (16).

При $P = 1$ используется обратное преобразование Лапласа выражения (17):

$$\varphi(t) = 1 - \lambda\sum_{i=1}^{n}(\lambda\mu)^{i-1}\beta_i(t), \tag{21}$$

$$\text{где } \beta_i(t) = \sum_{j=0}^{i-1} (-1)^j C_{i+j-1}^{i-1} \frac{t^{i-j-1}}{(i-j-1)!(\mu-\lambda)^{i+j}} (e^{-\lambda t} + (-1)^{i+j} e^{-\mu t}). \qquad (22)$$

Процедура определения значений ФЖ при использовании ДМП включает следующие основные этапы:

1. Определение и анализ исходных данных: прогнозируемого числа КА n, вероятности поражения ОИ при каждом воздействии P, ожидаемого времени ведения атак T, среднего времени до воздействия этой атаки m_η и среднего времени восстановления ОИ m_τ;
2. Обоснование целесообразности использования экспоненциальных законов распределения времени до воздействия и времени восстановления ОИ. Определение параметров этих законов $\lambda = 1/m_\eta$, $\mu = 1/m_\tau$;
3. Вывод аналитических соотношений или разработка алгоритмов определения значений ФЖ с помощью выражений (19), (20), (15), (16) при $P < 1$ или с помощью выражений (21), (22) при $P = 1$;
4. Определение значений ФЖ для конкретных количественных данных n, P, λ, μ.

Обсуждение результатов. Пусть дано, что число КА $n = 2$, интенсивность воздействий $\lambda = 1$, интенсивность восстановления $\mu = 2$, вероятность поражения $P = 0{,}5$, ожидаемое время ведения атак $T = 2$. Необходимо определить ФЖ и ее наименьшее значение, построить и сравнить графики функции для интенсивности воздействий $\lambda = 1, 2, 3, 4$.

В соответствии с формулами (19) и (20) общее выражение для ФЖ имеет вид:

$$\varphi(t) = 1 - \lambda P[\alpha_1(t) + \alpha_2(t)],$$

где $\alpha_1(t) = D_1 e^{-\lambda t} + B_1 e^{-\mu t}$, $\alpha_2(t) = t(D_2 e^{-\lambda t} + B_2 e^{-\mu t}) + D_1 e^{-\lambda t} + B_1 e^{-\mu t}$.

Коэффициенты D_1 и B_1 определяем для $\alpha_1(t)$ при условии $i = 1$. В результате получаем:

$$D_1 = (\mu - \lambda)^{-1}; \; B_1 = (\lambda - \mu)^{-1}.$$

Коэффициенты D_2, B_2, D_1, B_1 определяем для $\alpha_2(t)$ при условии $i = 2$. В результате получаем:

$$D_2 = (\mu - \lambda + P\lambda)(\mu - \lambda)^{-2}; \; B_2 = P\mu(\lambda - \mu)^{-2};$$
$$D_1 = [(\mu - \lambda)(1 - P) - 2(\mu - \lambda - P\lambda)](\mu - \lambda)^{-3}; \; B_1 = [(1 - P)(\lambda - \mu) - 2P\mu](\lambda - \mu)^{-3}.$$

Подставляем заданные значения λ, μ, P и полученные коэффициенты в общее выражение для ФЖ и после преобразований получаем:

$$\varphi(t) = 1 - 0{,}75(t - 1)e^{-t} - 0{,}5(t + 1{,}5)e^{-2t}.$$

Минимальное значение $\varphi_m \approx 0{,}83$ функция φ(t) принимает в точке $t_m \approx 1{,}04 < T$, поэтому имеем:

$$\inf_{t \in (0, T]} = \varphi(t_m) \approx 0{,}83.$$

Графики функций, составленные с использованием соответствующей компьютерной программы, изображены на рис. 2, шкала времени t имеет размерность часы. Шкала φ(t) имеет размерность вероятности. Из рис. 2 видно, что при неизменной интенсивности восстановления работоспособности ОИ ФЖ существенно уменьшается при возрастании интенсивности КА. При этом наименьшее значение ФЖ может составлять величину $\varphi_m \approx 0{,}64$ в случае $\lambda = 4$. Процедуру вывода соотношений для φ(t) можно упростить, используя предложенный ниже подход, основанный на суммировании взвешенных значений ФЖ при $P = 1$ и i-м сочетании из n воздействий и k поражений ОИ $\varphi_{ki}(t, P = 1)$, $k = 0, 1, 2, \ldots, n$. При этом сокращается объем промежуточных вычислений при определении коэффициентов D_{i-j} и B_{i-j}.

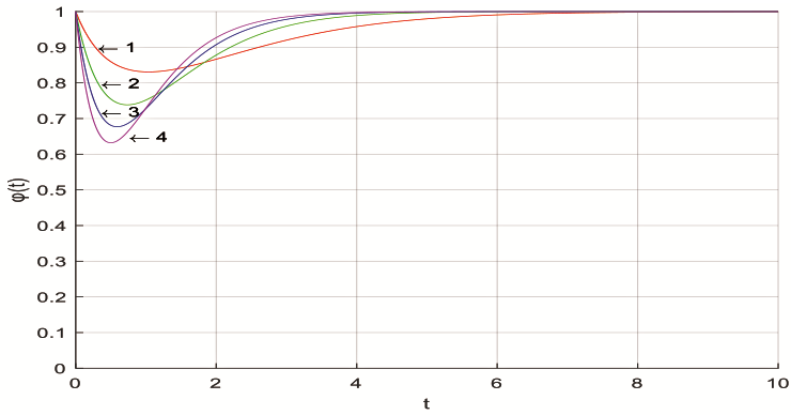

Рис.2. Графики функции живучести 1 - при λ = 1, 2 - при λ = 1, 3 - при λ = 3, 4 - при λ = 4
Fig.2. Graphs of the survivability function 1 - at λ = 1, 2 - at λ = 2, 3 - at λ = 3, 4 - at λ = 4

Так как каждому значению k соответствует m_k различных сочетаний возможных поражений и восстановлений ОИ из n по k, и вероятность каждого сочетания $P_k = P^k(1-P)^{n-k}$, то ФЖ выражается следующим образом:

$$\varphi(t) = \sum_{k=0}^{n} P_k \sum_{j=1}^{m_k} \varphi_{ki}(t, P=1) \ , \text{ где } m_k = C_n^k. \tag{23}$$

В том случае, если все n воздействий не приводят к поражению ОИ, то

$$\varphi_{01}(t, P=1) = 1.$$

Выражения для φ_{ki} определяются путем формирования соответствующих сочетаний k_i при заданном числе n воздействий и k поражений ОИ. Каждому сочетанию k_i будет соответствовать граф переходов (рис.3), где $z_j = 1$, $z'_j = 0$, $j = 1, 2, \ldots, k$; z_{k+1} – поглощающее состояние. Вероятности переходов равны единице, а функции распределения $F_j(t)$ времени пребывания процесса в состоянии $z_j = 1$ будут определяться числом воздействий противника n_j, которые он должен осуществить до j-го поражения ОИ.

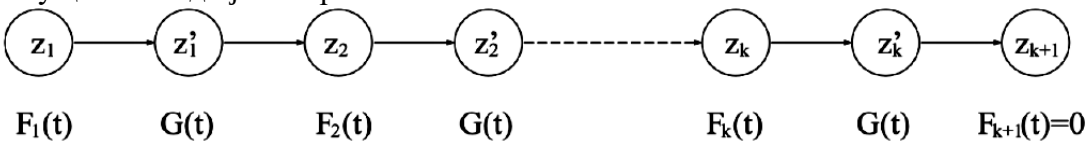

Рис.3. Граф переходов при P = 1
Fig.3. Transition graph for P = 1

В результате на основании нижеуказанного соотношения получаем (24):

$$\varphi(t, P=1) = 1 - \sum_{j=1}^{n} \left[F^{(j)}(t) * g^{(j-1)}(t) - F^{(j)}(t) * g^{(j)}(t)\right], \ g^{(0)}(t) = 1,$$

где знак «∗» обозначает операцию свертки функций, определяемую как

$$(F * g)(t) = \int_0^t F(t-\tau)g(\tau)d\tau, \ t \geq 0,$$

и где $g^{(j)}(t) = g * g^{(j-1)}$ – j-кратная свертка функции g, задается рекурсией;
$g(t) = G'(t)$ – плотность распределения времени восстановления;

$$\varphi(t, P=1) = 1 - \sum_{j=1}^{n} \left[F^{(n_j)}(t) * g^{(j-1)}(t) - F^{(n_j)}(t) * g^{(j)}(t)\right]; \ n_j = \sum_{s=1}^{j} r_s(k_i), \tag{24}$$

где n_j – суммарное число воздействий до j-го поражения ОИ; $r_s(k_i)$ – число КА после (s – 1)-го восстановления до s-го поражения ОИ, соответствующее сочетанию k_i.

На практике целесообразно выделить отдельные повторяющиеся (стандартные) соотношения в формулах для различных φ_{ki}, что позволяет упростить соответствующие компьютерные программы для вычисления. Например, используя соотношения F_1, F_2, F_3, F_4, F_5, F_6:

$$F_1 = F(t) - F(t) * g(t);\ F_2 = F^{(2)}(t) - F^{(2)}(t) * g(t);\ F_3 = F^{(3)}(t) - F^{(3)}(t) * g(t);$$
$$F_4 = F^{(2)}(t) * g(t) - F^{(2)}(t) * g^{(2)}(t);\ F_5 = F^{(3)}(t) * g(t) - F^{(3)}(t) * g^{(2)}(t);$$
$$F_6 = F^{(3)}(t) * g^{(2)}(t) - F^{(3)}(t) * g^{(3)}(t).$$

Тогда, применяя формулы (23) и (24), получаем:

$$\varphi(t, 1) = 1 - PF_1;$$
$$\varphi(t, 2) = 1 - P[F_1 + (1 - P)F_2] - P^2F_4;$$
$$\varphi(t, 3) = 1 - P\left[F_1 + (1 - P)F_2 + (1 - P)^2F_3\right] - P^2[F_4 + 2(1 - P)F_3]P^3F_6, \qquad (25)$$

где $\varphi(t, n)$ – ФЖ ОИ при n КА.

Выражения для F_i, i = 1, 2, …, 6, определяются путем выполнения соответствующих сверток функций F(t) и G(t). Для экспоненциальных законов распределения при $\mu \neq \lambda$ получаем:

$$F_1 = \lambda(\mu - \lambda)^{-1}(e^{-\lambda t} - e^{-\mu t});$$
$$F_2 = \lambda^2(\mu - \lambda)^{-2}\left\{[t(\mu - \lambda) - 1]e^{-\lambda t} + e^{-\mu t}\right\};$$
$$F_3 = \lambda^3(\mu - \lambda)^{-1}\left\{\left[0{,}5t^2 - t(\mu - \lambda)^{-1} + (\mu - \lambda)^{-2}\right]e^{-\lambda t} - (\mu - \lambda)^{-2}e^{-\mu t}\right\};$$
$$F_4 = \lambda^2\mu(\mu - \lambda)^{-2}\left\{\left[t - 2(\mu - \lambda)^{-1}\right]e^{-\lambda t} + \left[t + 2(\mu - \lambda)^{-2}\right]e^{-\mu t}\right\};$$
$$F_5 = \lambda^3\mu(\mu - \lambda)^{-2}\left\{\left[0{,}5t^2 - 2t(\mu - \lambda)^{-1} + 3(\mu - \lambda)^{-2}\right]e^{-\lambda t} - \left[t(\mu - \lambda)^{-1} + 3(\mu - \lambda)^{-2}\right]e^{-\mu t}\right\};$$
$$F_6 = \lambda^3\mu^2(\mu - \lambda)^{-3}(\left[0{,}5t^2 - 3t(\mu - \lambda)^{-1} + 6(\mu - \lambda)^{-2}\right]e^{-\lambda t} -$$
$$- \left[0{,}5t^2 + 3t(\mu - \lambda)^{-1} + 6(\mu - \lambda)^{-2}\right]e^{-\mu t}). \qquad (26)$$

При $\mu = \lambda$ функция F(t) = G(t), поэтому выражения для F_i, i = 1, 2, …, 6, принимают следующий вид:

$$F_1 = F(t) - F^{(2)}(t);\ F_2 = F^{(2)}(t) - F^{(3)}(t);\ F_3 = F_4 = F^{(3)}(t) - F^{(4)}(t);$$
$$F_5 = F^{(4)}(t) - F^{(5)}(t);\ F_6 = F^{(5)}(t) - F^{(6)}(t), \qquad (27)$$

где $F^{(n)}(t)$ – функция распределения Эрланга n-го порядка – закон распределения для композиции независимых случайных величин, распределенных по экспоненциальному закону: $F^{(n)}(t) = 1 - \sum_{i=0}^{n-1}(\lambda t)^i(i!)^{-1}e^{-\lambda t}$.

В результате, при $\mu = \lambda$ имеем:

$$F_1 = t\lambda(1!)^{-1}e^{-\lambda t};\ F_2 = (t\lambda)^2(2!)^{-1}e^{-\lambda t};\ F_3 = F_4 = (t\lambda)^3(3!)^{-1}e^{-\lambda t};$$
$$F_5 = (t\lambda)^4(4!)^{-1}e^{-\lambda t};\ F_6 = (t\lambda)^5(5!)^{-1}e^{-\lambda t}.$$

Путем введения идентификаторов для повторяющихся соотношений в формулах (26) и (27), например, для $e^{-\lambda t}$, $e^{-\mu t}$, $(\mu - \lambda)$ и т. д., и использования выражений (25) можно составить достаточно компактные компьютерные программы определения значений ФЖ для случаев экспоненциальных законов распределения F(t) и G(t). При этом параллельно требуется проверять условие исчерпания ресурса $R \leq R_0$. Если условие не выполняется, то считается, что процесс функционирования ОИ перешел в невозвратное состояние и требуется пополнение ресурса.

Вывод. Таким образом, результат исследований позволяет утверждать, что:

1. Задача оценки устойчивости ОИ в условиях КА имеет достаточную практическую значимость и востребована органами управления ИБ, что подтверждается апробацией на профильных конференциях;

2. Названную задачу и сопутствующие ей частные задачи можно выделить в особый однозначно определенный класс задач;

3. Выделенный класс задач, с учетом принятых ограничений, может быть представлен в виде соответствующих математических моделей.

Дальнейшие исследования планируется направить на разработку математической модели для оценки устойчивости функционирования ОИ в условиях КА: при произвольных законах распределения $F_i(t)$ и $G_i(t)$ и различных P_i. В этом случае процесс функционирования ОИ позиционируется как общий полумарковский процесс восстановления – это тема следующей публикации; при одинаковых законах распределения $F_i(t) = F(t)$ и $G_i(t) = G(t)$ и равных $P_i = P$. В этом случае процесс функционирования можно позиционировать как частный полумарковский – это тема также следующей публикации.

И в том, и в другом случаях новизна исследования будет определяться учетом при моделировании требуемого R_0 имеющегося ресурса R, выделенного для восстановления работоспособности ОИ после нанесения КА.

Библиографический список:

1. https://qrator.net/presentations/2021/QratorLabs_Network_Security_Availability_in_2020_RU.pdf[Visited March 20, 2022] Report on Network security and Availability in 2020 Available at.
2. Data Breach Investigations Report Available at: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf [Visited March 20, 2022].
3. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и защите информации" // СПС КонсультантПлюс.
4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 374-ст. М.: Стандартинформ, 2018. – 12 с.
5. Приказ ФСТЭК России от 29 апреля 2021 г. N 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. Зарегистрировано в Министерстве юстиции РФ 10 августа 2021 года, регистрационный N 64589. Электронный ресурс: https://docs.cntd.ru/document/608228209.
6. ГОСТ Р ИСО 19011–2021 Руководящие указания по проведению аудита систем менеджмента. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 21 апреля 2021 г. N261-ст. М.: Стандартинформ, 2021. – 42 с.
7. ГОСТ Р ИСО/МЭК 27007—2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 1.06.2015 М.: ФГУП «Стандартинформ», 2015. – 27 с.
8. ГОСТ Р 59516—2021. Информационные технологии. Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности. Утверж. и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. N420-ст. М.: Стандартинформ, 2021. – 20 с.
9. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. N 632-ст. М.: Стандартинформ, 2012 - 91 с.
10. Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1–29.
11. Лившиц И. И. Современная практика аудита информационной безопасности // Управление качеством. 2011. № 7. С. 34–41.
12. Кульба В. В., Шелков А. Б., Гладков Ю. М., Павельев С. В. Мониторинг и аудит информационной безопасности автоматизированных систем. – М.: ИПУ им. В. А. Трапезникова РАН, 2009. 94 с.
13. Марков А. С., Цирлов В. Л., Барабанов А. В. Методы оценки несоответствия средств защиты информации / под ред. А. С. Маркова. – М.: Радио и связь, 2012. 192 с.
14. Хохлачев Е. Н. Организация и технологии выработки решений при управлении системой и войсками связи. Часть 2. Выработка решений при восстановлении сетей связи. – М.: ВА РВСН, 2009. 241 с.
15. ГОСТ Р МЭК 61165-2019. Надежность в технике. Применение марковских методов. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 05 сентября 2019 г. N 635-ст. М.: Стандартинформ, 2019. 31 с.
16. ГОСТ Р 27.001-2009. Надежность в технике. Система управления надежностью. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. N 1247-ст. М.: Стандартинформ, 2010. 12 с.
17. Воеводин В. А., Маркин П. В., Маркина М. С., Буренок Д. С. Методика разработки программы аудита информационной безопасности с учетом весовых коэффициентов значимости свидетельств аудита на основе метода анализа иерархий // Системы управления, связи и безопасности. 2021. № 2. С. 96–129. DOI: 10.24412/2410-9916-2021-2-96-129.
18. Воеводин В. А., Буренок Д. С., Маркин П. В., Маркина М. С. «Программа метода анализа иерархий». Свидетельство о государственной регистрации программ для ЭВМ № 2020667542. Дата регистрации 24.12.2020.
19. V. A. Voevodin. Monte Carlo method for solving the problem of predicting the steadiness of the functioning of an automated control system in the conditions of massive computer attacks. Марчуковские научные чтения-2021: Тезисы Междунар. конф., 4–8 октября 2021 г. / Ин-т вычислит. математики и матем. геофизики СО РАН. С 75. DOI 0.24412/CL-35064-2021-095.

20. Надежность и эффективность в технике. Справочник Том № 5. Проектный анализ надежности/ под ред. В.И. Патрушева и А.И. Рембезы. – М.: Машиностроение, 1989, – 376 с.

References:

1. https://qrator.net/presentations/2021/QratorLabs_Network_Security_Availability_in_2020_RU.pdf[Visited March 20, 2022] Report on Network security and Availability in 2020 Available at.
2. Data Breach Investigations Report Available at: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf [Visited March 20, 2022].
3. Federal`ny` zakon ot 27.07.2006 N 149-FZ "Ob informacii, informacionny`h tehnologiyah i zashhite informacii" SPS *Konsul`tant Plyus.* (In Russ).
4. GOST R 51275–2006. Zashhita informacii. Ob``ekt informatizacii. Faktory`, vozdejstvuyushhie na informaciyu. Obshhie polozheniya: nacz. standart Ros. Federacii: izd. oficz.: utv. i vved. v dejstvie Prikazom Feder. agentstva po tehn. regulirovaniyu i metrologii ot 27 dekabrya 2006 g. № 374-st: vved. vpervy`e: data vved. 2021-11-30. M.: Standartinform, 2018; 8. (In Russ).
5. Prikaz FSTEK Rossii ot 29 aprelya 2021 g. N 77 On approval of the procedure for organizing and carrying out work on attesting informatization objects for compliance with the requirements for the protection of restricted information that is not a state secret. Registered with the Ministry of Justice of the Russian Federation on August 10, 2021, registration N 64589. Elektronnyj resurs: https://docs.cntd.ru/document/608228209. (In Russ).
6. GOST R ISO 19011–2021 Guidelines for auditing management systems. Approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated April 21, 2021 N261-st. M.: *Standartinform*, 2021; 42. (In Russ).
7. GOST R ISO/MEK 27007—2014. Information technology. Methods and means of ensuring security. Guidelines for auditing information security management systems. Approved and put into effect by order of the Federal Agency for Technical Regulation and Metrology dated 06/01/2015M.: FGUP «*Standartinform*», 2015; 27. (In Russ).
8. GOST R 59516—2021. Information Technology. Information security management. Information security risk insurance rules. Approval and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated May 20, 2021 N420-st.*M.: Standartinform*, 2021; 20. (In Russ).
9. GOST R ISO/MEK 27005-2010 Methods and means of ensuring security. Information security risk management. Approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated November 30, 2010 N 632-st.*M.: Standartinform*, 2012; 91. (in Russ).
10. Makarenko S. I. Audit of information security: main stages, conceptual framework, classification of measures. *Control Systems, Communications and Security*. 2018; 1: 1–29. (In Russ).
11. Livshic I.I. Modern practice of information security audit. *Quality management*. 2011;7:34–41. (In Russ).
12. Kul'ba V. V., SHelkov A. B., Gladkov YU. M., Pavel'ev S. V. Monitoring and audit of information security of automated systems. M.: IPU im. V. A. Trapeznikova RAN, 2009; 94. (In Russ).
13. Markov A. S., Cirlov V. L., Barabanov A. V. Methods for assessing the inconsistency of information security tools M.: *Radio and communication*. 2012; 192. (In Russ).
14. Hohlachev E. N. Organization and technology of making decisions in the management of the communication system and troops. Part 2. Development of solutions for the restoration of communication networks. M.: VA RVSN, 2009; 241 (in Russian).
15. GOST R MEK 61165-2019. Application of Markov methods. Approved and put into effect by the Order of the Federal Agency for Technical Regulation and Metrology dated Septembe N 635-st. M.: Standartinform, 2019; 31. (In Russ).
16. GOST R 27.001-2009. Nadezhnost' v tekhnike. Sistema upravleniya nadezhnost'yu. Utverzhden i vveden v dejstvie Prikazom Federal'nogo agentstva po tekhnicheskomu regulirovaniyu i metrologii ot 15 dekabrya 2009 g. N 1247-st. M.: Standartinform, 2010; 12. (In Russ).
17. Voevodin V. A., Markin P. V., Markina M. S., Burenok D. S. Technique for developing an information security audit program taking into account the weight coefficients of the significance of audit evidence based on the hierarchy analysis method. communications and security. *Sistemy upravleniya, svyazi i bezopasnosti.* 2021; 2: 96–129. DOI: 10.24412/2410-9916-2021-2-96-129. (In Russ).
18. Voevodin V. A., Burenok D. S., Markin P. V., Markina M. S. «Programma metoda analiza ierarhij». Svidetel'stvo o gosudarstvennoj registracii programm dlya EVM № 2020667542. Data registracii 24.12.2020. (In Russ).
19. V. A. Voevodin. Monte Carlo method for solving the problem of predicting the steadiness of the functioning of an automated control system in the conditions of massive computer attacks. Marchuk Scientific Readings-2021: Abstracts of the Intern. Conf., October 4–8, 2021; 75. *Institute of Comput. mathematics and math. geophysics SB RAS.* DOI 0.24412/CL-35064-2021-095.
20. Reliability and efficiency in technology. Handbook Volume No. 5. Design reliability analysis / ed. IN AND. Patrushev and A.I. Rembeza. *Mashinostroenie.* 1989; 376. (In Russ).

Сведения об авторах:
Воеводин Владислав Александрович, кандидат технических наук, доцент кафедры информационной безопасности; vva541@mail.ru
Виноградов Иван Вадимович, студент; кафедра информационной безопасности; ivanvinogradov1111@gmail.com
Волков Даниил Игоревич, студент; кафедра информационной безопасности; d.i.volkov2002@mail.ru
Information about authors:
Vladislav A. Voevodin, Cand.Sci. (Eng.), Assoc. Prof., Department of Information Security; vva541@mail.ru
Ivan V. Vinogradov, STudent; Department of Information Security; ivanvinogradov1111@gmail.com
Daniil I. Volkov, Student; Department of Information Security; d.i.volkov2002@mail.ru

Конфликт интересов/Conflict of interest.
Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.
Поступила в редакцию/Received 29.08.2022.
Одобрена после рецензирования/ Reviced 20.09.2022.
Принята в печать/Accepted for publication 20.09.2022.