УДК 004.056 **DOI** 10.15622/ia.22.3.8

В.А. Воеводин

МОДЕЛЬ ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ ЭЛЕМЕНТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ДЛЯ УСЛОВИЙ ВОЗДЕЙСТВИЯ МНОЖЕСТВА КОМПЬЮТЕРНЫХ АТАК

Воеводин В.А. **Модель оценки функциональной устойчивости элементов информационной инфраструктуры для условий воздействия множества компьютерных атак.**

Аннотация. Приводятся сведения о новом подходе к приложению методов теории полумарковских процессов для решения прикладной задачи по оцениванию функциональной устойчивости элементов, входящих в состав информационной инфраструктуры, функционирующей в условиях воздействия множества компьютерных атак. Задача оценивания функциональной устойчивости сводится к задаче поиска функции живучести исследуемого элемента и определению ее экстремальных значений. Обосновывается актуальность исследования. В основе обоснования лежит предположение о том, что количественные методы исследования устойчивости технических систем, которыми оперирует теория надежности, не всегда могут быть применены для оценки живучести. Уточняются понятия «устойчивость» и «компьютерная атака». Формулируются вербальная и формальная постановки задач исследования. Новизна полученных результатов заключается в применении известных методов для решения практически значимой задачи в новой постановке с учетом ограничения на ресурс, выделенный для поддержания живучести исследуемого элемента, при условии принятия произвольных законов распределения случайных времен реализации компьютерных атак и времен восстановления функционала элемента. Приводятся рекомендации по формированию исходных данных, содержание укрупненных этапов моделирования и тестовый пример для демонстрации работоспособности модели. Приводятся результаты тестового моделирования в виде графиков функции живучести. Полученное приложение может быть использовано на практике для построения функции живучести при реализации до трех компьютерных атак, а также как инструмент для оценивания достоверности аналогичных статистических моделей. Ограничение объясняется прогрессивным возрастанием размерности аналитической модели и снижением возможности её содержательной интерпретации.

Ключевые слова: информационная инфраструктура, элемент информационной инфраструктуры, функциональная устойчивость, функция живучести, компьютерная атака, аудит информационной безопасности, полумарковские процессы, угрозы информационной безопасности.

1. Введение. Отношения в области обеспечения устойчивости функционирования информационной инфраструктуры (ИИ) в условиях компьютерных атак регулируются федеральными законами: а) от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» б) от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и сопутствующими им подзаконными актами.

Сведения о динамике компьютерных атак, которые сопровождают эти отношения, приведены в [1 – 3]. Эффективное регулирование таких отношений возможно, если органы управления обладают инструментом, позволяющим своевременно и достоверно оценить устойчивость функционирования соответствующей ИИ.

Такой инструмент может быть востребован:

1. Лицами, управляющими программой аудита информационной безопасности (ИБ), при разработке программы и методик аудита.
2. Органами управления ИБ при обеспечении устойчивости функционирования ИИ в условиях КА для:
   - а. выработки требований к устойчивости при взаимодействии с заказчиком;
   - б. прогнозирования обстановки, которая может сложиться в условиях воздействия угроз ИБ;
   - в. оценки эффективности системы восстановления функциональности ИИ;
   - г. обоснования решения при подготовке предложений по бюджетированию мер обеспечения ИБ.
3. Лицами, осуществляющими оценивание рисков ИБ с целью обоснования страховых тарифов (в перспективе).

Официального определения понятия «устойчивость» применительно к ИИ в нормативных правовых актах не приводится, поэтому за основу взято адаптированное определение, приведенное в [4]. Таким образом, под функциональной устойчивостью ИИ («функциональная устойчивость») понимается ее способность сохранять либо своевременно восстанавливать требуемую функциональность в различных условиях обстановки.

Также уточнено понятие «компьютерная атака» (КА) – воздействие угроз нарушения информационной безопасности на элементы информационной инфраструктуры объекта информатизации, направленное на уничтожение, раскрытие, изменение, блокирование, кражу, получение несанкционированного доступа к информации. Целью КА могут быть элементы различной природы, например технические средства, программные средства, человек, группы людей, которые в результате успешной атаки теряют требуемый функционал. Поэтому это понятие несколько шире по объему, чем приведенное в федеральном законе от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», ст. 2, п. 4.

Для оценивания функциональной устойчивости ИИ в целом требуются исходные данные, содержащие оценки устойчивости функционала отдельных элементов, входящих в состав ИИ. Отдельные элементы ИИ (Элементы) рассматриваются без учета их внутренней структуры, физической природы и места в составе ИИ.

Для штатных условий имеется потенциальная возможность добыть репрезентативную статистику частных показателей устойчивости, что позволяет использовать для оценивания устойчивости Элементов количественные методы теории надежности. Другими словами, случайные явления, сопровождающие процесс применения, носят стохастическую неопределенность, что позволяет использовать асимптотические оценки соответствующих показателей. Зная оценки устойчивости отдельных Элементов в штатных условиях применения, представляется возможным оценить для этих же условий функциональную устойчивость ИИ в целом. Результаты фундаментальных исследований в области теории надежности сложных технических систем приведены в [5, 6]. Приложению методов теории надежности для оценки устойчивости технических систем, функционирующих в штатных условиях, посвящены публикации российских и зарубежных исследователей [7 – 13]. Таким образом, результаты ретроспективного анализа имеющейся литературы позволяют утверждать, что сегодня имеется достаточный научный задел для решения задачи оценивания функциональной устойчивости элементов ИИ для штатных условий ее применения.

Для условий нештатного применения репрезентативная статистика отсутствует в принципе, что порождает ряд особенностей при оценке функциональной устойчивости ИИ. Такая ситуация связана, прежде всего, с тем, что сами нештатные условия порождены воздействием угроз ИБ. Воздействия угроз можно позиционировать как редкие явления, их длительность непредсказуема, сама обстановка при нештатных условиях весьма нестабильна, а неопределенность часто носит поведенческий характер. В этих условиях процессы исследуемых событий нельзя принять ни стационарными, ни эргодическими, ни стохастическими. Названные особенности не позволяют в полной мере применить классические методы математической статистики и теории вероятностей. Для решения задачи требуется разработка специальных методов оценки функциональной устойчивости с учетом вышеназванных особенностей. Разработке специальных подходов к определению функциональной устойчивости случайных явлений нестохастической природы для оценивания устойчивости критической инфраструктуры

посвящены публикации [14 – 33]. Однако в названных публикациях при моделировании не учитываются ограничения на ресурс, который имеется для восстановления функциональности Элемента.

2. Постановка задачи. Пусть задана некая ИИ объекта информатизации, содержащая семейство взаимоувязанных Элементов. Информационная инфраструктура, в состав которой входят отдельные Элементы, подвергается КА. На этапе проектирования ИИ для каждого из Элементов были реализованы специальные меры, обеспечивающие некую их защищенность от КА. Более того, в ставе ИИ имеется система восстановления ее функционала, обладающая неким производственным потенциалом (ресурсом). Система восстановления реагирует на поражение ИИ посредством восстановления пораженных Элементов, в результате чего восстанавливается ее функционал. При этом расходуется соответствующий ресурс системы восстановления.

Допущение. Для решения задачи принято допущение, суть которого заключается в том, что функция устойчивости Элемента на заданном интервале времени (0, T] реализации КА представляется в виде композиции двух независимых функционалов. Эта композиция имеет вид:

$$\nu\left(t, u, \Delta T, \lambda, \mu, \boldsymbol{P}\right) = K_{\text{ОГ}}\left(t, u, \Delta T\right)\varphi\left(t, \lambda, \mu, \boldsymbol{P}\right), \qquad (1)$$

где $\nu(t, u, \Delta T, \lambda, \mu, \boldsymbol{P})$ – функция устойчивости Элемента;

t – временной параметр оценки функции устойчивости;

u – показатель безотказности и восстанавливаемости Элемента в штатных условиях применения, $u = \{T_{\text{н}}, T_{\text{в}}\}$, где $T_{\text{н}}$ – средняя наработка на отказ Элемента в штатных условиях; $T_{\text{в}}$ – среднее время восстановления работоспособности Элемента. Значения частных показателей возможно получить на основе обработки соответствующих статистических данных, полученных в штатных условиях применения или из эксплуатационной документации;

ΔT – период времени от начала до окончания воздействий КА;

$\lambda = \{\boldsymbol{F}, n, T\}$ – характеристика КА, где $\boldsymbol{F}$ – совокупность функций распределения случайных интервалов времени η_i до очередной i-й КА, $\boldsymbol{F} = \{F_i(t)\}$, где $F_i(t)$ – функция распределения случайного η_i интервала времени до i-й КА, $i = 1, 2, \ldots, n$, n – количество КА, T – момент времени окончания воздействий угроз информационной безопасности (КА);

μ – частный показатель живучести Элемента, характеризующий его способность восстанавливать нарушенный в результате успешных

КА функционал, $\mu = \{\boldsymbol{T}_в, \boldsymbol{G}\}$, где $\boldsymbol{T}_в = \{\tau_{вi}^н, \tau_{вi}^в\}$ – совокупность нижнего и верхнего интервалов времени восстановления функционала;

$\boldsymbol{G}$ – совокупность функций распределения случайных интервалов времени восстановления функционала Элемента после i-й КА, $\boldsymbol{G} = \{G_i(t)\}$, $i = 1, \ldots, n$, n – число КА, $\tau_{вi}^н$ – оценка нижнего интервала восстановления функционала после i-й КА, $\tau_{вi}^в$ – оценка верхнего интервала восстановления функционала после i-й КА. Оценка параметров $\{\tau_{вi}^н, \tau_{вi}^в\}$ осуществляется либо с помощью экспертных методов, либо в результате соответствующих учений, деловых игр или специальных исследований [34, 35];

$\boldsymbol{P}$ – совокупность частных показателей живучести Элемента, характеризующая его защищенность, т.е. способность сохранять требуемый функционал в результате отражения КА. В качестве такого показателя принята совокупность вероятностей поражения Элемента при отражении КА, $\boldsymbol{P} = \{p_i\}$, где p_i – вероятность поражения Элемента при i-й КА, $i = 1, \ldots n$, n – число КА. Оценка вероятностей p_i осуществляется либо с помощью экспертных методов, либо добывается в результате соответствующих учений, деловых игр или статистического моделирования;

$K_{ОГ}(u, t) = K_Г(u)\, P(t, \Delta T)$ – нестационарный коэффициент оперативной готовности Элемента, определяемый вероятностью его безотказной работы в течение времени реализации КА и устранения ее последствий, $\Delta T = (0, T]$, где $K_Г(u)$ – коэффициент готовности Элемента, рассчитанный для штатных условий его применения, $P(t, \Delta T)$ – вероятность безотказной работы Элемента в течение периода времени ΔT;

$\varphi(t, \lambda, \mu, \boldsymbol{P})$ – функция живучести Элемента в условиях КА.

Для большинства практических случаев значение $K_{ОГ}(u)$ на периоде времени ΔT очень близко к единице, а значение функции живучести на этом же периоде неизмеримо меньше $\varphi(t, \lambda, \mu, \boldsymbol{P}) << K_{ОГ}(u)$ [17]. С учетом этого утверждения формулу (1) можно привести к виду:

$$\nu(t, \lambda, \mu, u, \boldsymbol{P}) \approx \varphi(t, \lambda, \mu, \boldsymbol{P}),$$

т.е. функция устойчивости Элемента, для условий КА, может быть приближенно заменена функцией живучести.

В качестве показателей, характеризующих функцию живучести, предлагается использовать показатели, характеризующие

экстремальные значения функции живучести, не зависящие от времени. Например, такими показателями могут быть:

а. наименьшее значение функции живучести Элемента на заданном интервале времени $(0, T]$, $\varphi_m = \min\limits_{t\in(0,\,T]} \varphi\left(t, \lambda, \mu, \boldsymbol{P}\right)$;

б. среднее значение функции живучести Элемента на заданном интервале времени $(0, T]$: $\varphi_{\text{с}} = \dfrac{1}{T}\int\limits_0^T \varphi\left(t, \lambda, \mu, \boldsymbol{P}\right) dt$;

в. коэффициент живучести Элемента, характеризующий вероятность состояния «функционален» в любой произвольный момент времени $t\in(0, T]$: $k_\varphi = \lim\limits_{\substack{t\to T\\ n\to N}} \varphi\left(t, \lambda, \mu, \boldsymbol{P}\right)$, где T – прогнозируемый максимальный момент времени реализации множества КА, который определяется с помощью экспертных методов; N – максимальное прогнозируемое число КА в составе множества, которое также определяется с помощью экспертных методов.

Ранее автором исследовалась возможность решения подобной задачи с помощью статистического моделирования методом Монте-Карло. Были получены положительные результаты, авторский подход к моделированию приведен в [32, 33]. При этом исходные данные для моделирования добывались экспертными методами. Кроме экспертных методов источником исходных данных могут быть результаты учений, деловых игр или специальные методы исследований [34]. Применение методов статистического моделирования весьма ресурсоемко с точки зрения времени. Время моделирования может быть сравнимо с периодом КА, что отрицательно сказывается на своевременности оценки, которая просто может потерять свою актуальность. Также проблемным является вопрос оценки достоверности получаемых результатов статистического моделирования, для этого требуются альтернативные методы оценивания.

В этой связи возникает резонный вопрос: а возможно ли построить аналитическую (математическую) модель, которая по добытым исходным данным позволила бы посредством математических расчетов получить оценку функции живучести Элемента для условий КА? Для получения ответа на этот вопрос была исследована возможность применения методов теории полумарковских процессов.

В [17, 30, 31] приведены фундаментальные основания для приложения общих марковских потоков событий, и показана их связь с марковскими аддитивными процессами и процессами марковского

восстановления, рассмотрены важные для их практических приложений частные случаи таких потоков. Анализ публикаций на обозначенную тему позволяет утверждать, что вопросам практического применения методов теории полумарковских процессов посвящено значительное число работ [37 – 43]. Результаты ретроспективного исследования названных публикаций позволяют утверждать, что в основном предлагается подход, основанный на асимптотических оценках устойчивости, что не может являться не спорным. Моделируемые процессы, без грубых допущений, нельзя принять стационарными, следовательно, усредненные исходные данные могут давать значительную погрешность в оценках устойчивости. Плюс к этому за пределами предмета публикаций осталась конкретизация методов теории полумарковских процессов для условий ограничения на ресурс, с помощью которого поддерживается сам полумарковский процесс. При этом не учитывается возможность перехода полумарковского процесса в невозвратное состояние по исчерпанию ресурса.

Уточненная задача оценивания живучести Элемента к КА с учетом имеющегося ресурса формулируется следующим образом: конкретизировать постановку задачи (1) с учетом ограничений на имеющийся, для обеспечения живучести Элемента, ресурс в условиях КА.

При уточнении, формальная постановка задачи (1) конкретизируется и приобретает вид:

$$\nu\left(t, \Delta T, u, \lambda, \mu, \boldsymbol{P}, \Pi_0, \Pi^{\text{Тр}}\right) = K_{\text{ОГ}}\left(t, \Delta T, u\right)\varphi\left(t, \lambda, \mu, \boldsymbol{P}, \Pi_0, \Pi^{\text{Тр}}\right),$$

где частный план восстановления функционала Элемента должен удовлетворять следующим ограничениям:

$$\boldsymbol{\Pi}^* = \left\{\pi^*\right\} = \left\{\boldsymbol{R}^{\text{Тр}} \le \boldsymbol{R}_0, \boldsymbol{D}^{\text{Тр}} \le \boldsymbol{D}_0\right\},$$

где $\boldsymbol{\Pi}^*=\{\pi^*\}$ – совокупность альтернативных планов восстановления функционала Элемента, удовлетворяющих ограничениям на ресурс.

При этом:

а) Π_0 – показатель, характеризующий требуемые производственные возможности подсистемы восстановления функционала:

$$\Pi_0 = \{\boldsymbol{R}_0, \boldsymbol{D}_0\},$$

где $\boldsymbol{R}_0 = \{r_{0i}\}$ – совокупность типов расходуемого ресурса, имеющегося в составе системы восстановления функционала для восстановления Элемента, $i = 1, 2, \ldots, m$; m – число типов расходуемого ресурса (пример расходуемого ресурса – запасные части, расходный материал и т.п.); $\boldsymbol{D}_0 = \{d_{0i}\}$ – совокупность типов возобновляемого ресурса, имеющегося в составе системы восстановления функционала, $i = 1, 2, \ldots, k$, k – число типов возобновляемого ресурса (пример возобновляемого ресурса – люди, измерительные приборы и т.п., которые могут использоваться многократно);

б) показатель, характеризующий требуемые производственные возможности расчета восстановления: $\Pi^{\text{Тр}} = \left\{\boldsymbol{R}^{\text{Тр}}, \boldsymbol{D}^{\text{Тр}}\right\}$, показатель, характеризующий требуемые производственные возможности расчета восстановления, где $\boldsymbol{R}^{\text{Тр}} = \left\{r_i^{\text{Тр}}\right\}$ – совокупность соответствующих единиц расходуемого ресурса каждого типа, требуемых для восстановления функционала Элемента после успешной КА, $i = 1, 2, \ldots, m$, m – число требуемых типов расходуемого ресурса; $\boldsymbol{D}^{\text{Тр}} = \left\{r_i^{\text{Тр}}\right\}$ – совокупность типов возобновляемого ресурса, требуемого для восстановления функционала, $i = 1, 2, \ldots, k$, k – число требуемых типов возобновляемого ресурса.

Поставленная задача решалась в два этапа:

1) определение оператора A: $\varphi(t)=A\{t, \Delta T, \boldsymbol{F}, \boldsymbol{G}, \boldsymbol{P}, n, \Pi_0, \Pi^{\text{Тр}}\}$;

2) определение минимума функционала $\varphi_{\text{m}} = \min\limits_{t\in(0,\,T]} \varphi\left(t, \Delta T, \lambda, \mu, \boldsymbol{P}, \Pi_0, \Pi^{\text{Тр}}\right)$.

Наиболее сложным, неоднозначным и неформализуемым является этап обоснования выбора оператора для совокупности произвольных законов распределения $\boldsymbol{F} = \{F_i(t)\}$ и $\boldsymbol{G} = \{G_i(t)\}$ и различных вероятностей поражения Элемента при КА, $\boldsymbol{P} = \{P_i\}$.

Требования к обеспечению живучести нормированы в подзаконных актах к соответствующим федеральным законам и в соответствующих нормативных правовых документах. При моделировании учитывалось ограничение на имеющийся ресурс для восстановления функционала Элемента в условиях КА, для чего было введено понятие невозвратного состояния Элемента, в которое он может перейти из-за исчерпания ресурса, выделенного для восстановления его функционала.

Для моделирования процесс функционирования Элемента был представлен в виде иерархического ориентированного графа типа

дерева, содержащего одну начальную z_1 и m конечных вершин (рисунок 1).

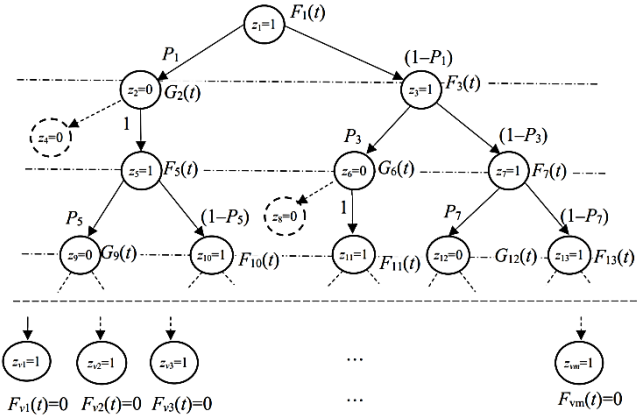

Рис. 1. Граф переходов процесса восстановления функционала Элемента для условий КА

Начальной вершине графа соответствует момент начала множества КА и состояние Элемента «функционален»: $t_0 = 0$, $z_1 = 1$ («функционален»). Через случайный промежуток времени $(t_0 + \eta_1)$, распределенный по закону $F_1(t) = P\{(t_0 + \eta_1) < t\}$, Элемент подвергается КА. В результате КА он может быть поражен с вероятностью P_1 или не поражен с вероятностью $(1 - P_1)$. Если КА была успешной, то Элемент в момент времени $(t_0 + \eta_1)$ переходит в состояние $z_2 = 0$ («не функционален») и начинается процесс восстановления его функционала, при этом расходуется соответствующий ресурс $\Pi^{\text{Тр}} = \left\{\boldsymbol{R}^{\text{Тр}}, \boldsymbol{D}^{\text{Тр}}\right\}$. В результате восстановления функциональности Элемента, через случайный период времени τ_2, он возвращается в состояние «функционален». Случайный период времени τ_2 распределен по закону $G_2(t) = P\{(t_0 + \eta_1 + \tau_2) < t\}$, при этом расходуется соответствующий, фиксированный для каждого восстановления, ресурс $\Pi^{\text{Тр}} = \left\{\boldsymbol{R}^{\text{Тр}}, \boldsymbol{D}^{\text{Тр}}\right\}$.

В результате восстановления Элемент переходит в состояние $z_5 = 1$ и вновь подвергается, через случайный период времени η_5, очередной КА. При этом случайный период времени η_5 распределен по закону $F_5(t) = P\{(t_0 + \eta_1 + \tau_2 + \eta_5) < t\}$ и т.д. Если Элемент в результате первой КА сохранит функциональность, он переходит

в новое состояние $z_3 = 1$, которое отличается от состояния $z_1 = 1$ другой вероятностью поражения P_3 или непоражения $(1 - P_3)$. При учете ограничений на ресурс случайный процесс может быть завершен невозвратными состояниями (на рисунке 1 это z_4 и z_8). Для восстановления функциональности Элемента требуется соответствующий ресурс:

$$\Pi^{\text{Тр}} = \left\{ \sum_{i \in M_+} r_{ij}^{\text{Тр}} \le R_{0j}, \max_{i \in M_+} d_j^{\text{Тр}}(t) \le d_{0j}(t) \right\}, \quad (2)$$

где M_+ – множество успешных КА; $r_{ij}^{\text{Тр}}$ – требуемый для восстановления функциональности Элемента расходуемый ресурс j-го вида, при i-й успешной КА; R_{0j} – имеющийся расходуемый ресурс j-го вида.

Таким образом, суммарный израсходованный ресурс $\sum_{i \in M_+} r_{ij}^{\text{Тр}}$ не должен превышать имеющийся – R_{0j}, в противном случае процесс переходит в невозвратное состояние «не функционален» по исчерпанию ресурса.

Максимальная потребность в возобновляемом ресурсе в текущий момент времени $\max_{i \in M_+} d_j^{\text{Тр}}(t)$ не должна превышать имеющийся на этот же момент времени возобновляемый ресурс $d_{0j}(t)$. Иными словами, один и тот же прибор или специалист не должен применяться в одно и то же время в разных местах. В противном случае процесс переходит в невозвратное состояние. В результате невозвратным вершинам могут соответствовать и промежуточные состояния полного графа (на рисунке 1 это z_4 и z_8), в которых Элемент так и останется в состоянии $z_i = 0$. Поэтому актуальными частными задачами при оценке живучести Элемента являются:

а. оценка вероятности того, что в момент времени t Элемент будет поражен, но не будет восстановлена его функциональность из-за исчерпания ресурса, определяемая неравенством (2);

б. оценка минимального значения функции живучести $\varphi_{\text{m}} = \min_{t \in (0,T]} \varphi(t)$, а также времени наступления этого минимума t_m.

Начальную вершину z_1 и каждую конечную вершину z_{vi} соединяет путь, содержащий вершины, которым сопоставлены соответствующие состояния Элемента, а ребрам сопоставлены вероятности перехода в эти состояния. Каждому состоянию z_i соответствует функция распределения $F_i(t)$ случайного времени реализации i-й КА – η_i. При этом с вероятностью P_i, $z_i = 0$, если i-я КА была успешной, и $(1 - P_i)$, $z_i = 1$, если i-я КА была неуспешной. Состояние $z_{vi} = 1$, где v – индекс конечной вершины и соответствует окончанию множества КА при условии, что имеющегося ресурса будет достаточно $\Pi^{\text{Тр}} \geq \Pi_0$.

Индексы j всех последующих состояний $z_j = 1$ превышают индексы i предыдущих состояний, $j > i$. Число вершин графа соответствующих состояний Элемента будет однозначно зависеть от числа КА – n. При этом общее число возможных состояний Элемента $M_0 = 3 \cdot 2^n - 2$ (выведено эмпирически без строгого доказательства). Число поглощающих состояний $m = 2^n$. Число k_+ состояний $z_i = 1$ и число k_- состояний $z_i = 0$, без учета поглощающих состояний, равны $k_+ = k_- = 2^n - 1$.

При поиске решения были приняты следующие допущения:

а. вероятность перехода π_{ij} из состояния z_i в состояние z_j на каждом пути зависит только от состояния z_i и не зависит от предыстории процесса, т.е. пути к состоянию z_i, т.е. принимаем, что процесс обладает свойством «без последействия»;

б. случайные величины η_i и τ_i и их законы распределения независимы;

в. процесс восстановления завершается в случае, если закончился соответствующий ресурс (2), процесс переходит в невозвратное состояние и Элемент остается в состоянии $z = 0$ (на рисунке 1 это состояния под номерами z_4, z_8). Из невозвратного состояния процесс может выйти только при получении дополнительного ресурса;

г. процесс переходит в поглощающее состояние с $z_{vi} = 1$, в силу прекращения КА.

Таким образом, для определения оператора A при произвольных законах распределения $F_i(t)$ и $G_i(t)$, заданных вероятностях поражения P_i и ограничениях на ресурс (2) представляется возможным применить полумарковскую модель процесса восстановления функциональности Элемента в условиях ограничения на ресурс. Модель описывается ступенчатым случайным процессом, который задается:

а. вероятностями перехода π_{ij};

б. законами распределения времени пребывания процесса в каждом из состояний $F_i(t)$ и $G_i(t)$;

в. ограничением (2).

При моделировании следует учитывать особенности процесса:

1. Процесс не является эргодическим, т.к. он содержит множество невозвратных и поглощающих состояний, что не позволяет применить асимптотические оценки случайных величин τ_i и η_i.

2. Длительность совокупности последовательных КА имеет конечное значение, что также препятствует применению асимптотических оценок для оценки живучести Элемента.

3. При построении графа учитываются ограничения на ресурс (2).

4. Вероятность перехода π_{ij} из состояния z_i в состояние z_j принимает следующие значения:

– $\pi_{ij} = 0$, если $i \geq j$ или если z_i и z_j не являются смежными вершинами;

– $\pi_{ij} = P_i$, если $z_i = 1$ и $z_j = 0$;

– $\pi_{ij} = 1 - P_i$, если $z_i = z_j = 1$;

– $\pi_{ij} = 1$, если $z_i = 0$ и $z_j = 1$.

5. Условная функция распределения $F_{ij}(t)$ времени пребывания процесса в любом i-м состоянии равна безусловной функции распределения времени пребывания процесса в этом состоянии. Действительно, состоянию $z_i = 1$, из которого возможен переход в состояние $z_- = 0$ с вероятностью P_i при поражении Элемента или в состояние $z_+ = 1$ с вероятностью $(1 - P_i)$ при непоражении Элемента, соответствует безусловная функция распределения $F_i(t)$, определяемая с помощью известного [6, 17, 30] выражения $F_i(t) = P_i F_{i-}(t) + (1 - P_i) F_{i+}(t)$, где функция распределения $F_{i-}(t)$ случайного времени перехода из состояний z_i в состояние $z = 0$ при реализации i-й КА; P_i – вероятность поражения Элемента при реализации i-й КА; $F_{i+}(t)$ – функция распределения случайного времени перехода из состояний z_i в состояние $z = 1$ при реализации i-й КА. Учитывая, что закон распределения времени до i-й КА не зависит от поражения Элемента в результате предшествующих КА, справедливо равенство $F_{i-}(t) = F_{i+}(t)$, поэтому $F_i(t) = F_{i-}(t)$. Состоянию $z_i = 0$ будет также соответствовать одна и та же функция распределения: $G_i(t) = G_{i+}(t)$, т.к. переход из этого состояния осуществляется с вероятностью $\pi_{i+} = 1$, за исключением случая, когда будет исчерпан ресурс для восстановления функциональности Элемента. В этом случае процесс перейдет в поглощающее состояние по исчерпанию ресурса.

3. Решение задачи. Для моделирования было выделено множество индексов N_+ состояний элемента $z_i = 1$, $i \in N_+$, и множество индексов N_- состояний $z_j = 0$, $j \in N_-$. Очевидно, что функция живучести, характеризующая вероятность нахождения Элемента в состоянии «функционален» в момент времени t, будет равна сумме вероятностей $P_{1i}(t)$ нахождения Элемента в состояниях, имеющих индексы N_+, при условии, что в начальный момент времени $t_0 = 0$ он находился в состоянии $z_i = 1$, т.е.:

$$\varphi(t) = \sum_{\substack{i \in N_+ \\ \Pi^{\text{Тр}} \le \Pi_0}} P_{1i}(t), \tag{3}$$

где N_+ – множество индексов $N_+ = 2^{n+1} - 1$, соответствующих состоянию Элемента «функционален».

Вероятности $P_{1i}(t)$ позиционируются как интервально-переходные, которые определяются с помощью системы линейных интегральных уравнений. Сама идея математического моделирования для стационарных условий и при отсутствии ограничений на ресурс приведена в [17, 30]:

$$P_{1i}(t) = \left[1 - F_1(t)\right]\delta_{1i} + \sum_{k \in N_+} \pi_{1k} \int_0^t f_{1k}(\tau)\, g_{ki}(t-\tau)\, d\tau; \tag{4}$$

$$g_{ki}(t-\tau) = \left[1 - F_k(t)\right]\delta_{ki} + \sum_{r \in N_-} \pi_{kr} \int_0^t f_{kr}(\tau)\, g_{ri}(t-\tau)\, d\tau, \tag{5}$$

где $i \in N_+$; $k, r \in N_-$; $\delta_{ki} = 1$ при $k = i$; $\delta_{ki} = 0$ при $k \ne i$; $f_{1k}(\tau)$ и $f_{kr}(\tau)$ – условные плотности распределения случайного времени пребывания Элемента в состоянии z_1 и z_k соответственно; $N = N_+ \cup N_-$ – совокупность индексов всех возможных состояний Элемента. Значения $g_{ki}(t-\tau)$ определяются по формуле (5).

Первый член в уравнении (4) определяет вероятность того, что Элемент останется в состоянии z_1 до момента времени t. Второй член в (4) – вероятность последовательности событий перехода Элемента из z_1 в z_k к моменту τ и из состояния z_k в состояние z_i за оставшееся время $(t - \tau)$. Вероятности частных переходов суммируются по всем промежуточным состояниям z_k, в которые возможны переходы

из начального состояния z_1, и интегрируются по всем возможным временам перехода τ между 0 и t.

Для снижения сложности процедуры определения функции живучести во временно̀й шкале параметра функции применялось преобразование Лапласа. Таким образом, процедура определения оператора A включала следующие шаги:

1. определение совокупности возможных состояний Элемента $\boldsymbol{Z} = \{z_i\}$, $i = 1, 2, \ldots, M_0$, $M_0 = 1, 2, \ldots, 3 \cdot 2^n - 2$ и построение полного графа переходов;

2. определение совокупности индексов $N_+ = \{z_i = 1\}$, $i = 1, 2, \ldots, m_+$, где $m_+ = 2^{n+1} - 1$;

3. построение соотношений для интервально-переходных вероятностей $P_{1i}(t)$, $i \in N_+$ с использованием выражений, полученных в результате преобразований Лапласа и соответствующих таблиц преобразований;

4. определение общего выражения для функции живучести $\varphi(t)$ с использованием формулы (3).

Для отображения самой предлагаемой идеи получения аналитического выражения функции живучести $\varphi(t)$ ниже приводятся два тестовых примера ее выведения.

Процедура аналитического вычисления $P_{1i}(t)$ весьма громоздкая, поэтому рекомендуется подходить к применению метода взвешенно в каждом конкретном случае при относительно небольшом числе воздействий. Для произвольного числа воздействий рекомендуется применять соответствующие программы для ЭВМ, реализующие числовые методы или методы статистического моделирования. Представляет интерес применение метода Монте-Карло. Идея и результат применения этого метода апробированы автором, результаты приведены в [32, 33].

4. Тестовый пример. Пусть число КА $n = 1$. Требуется определить функцию живучести Элемента $\varphi(t)$. Множество состояний Элемента и граф переходов представлен на рисунке 2.

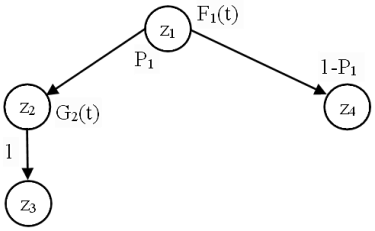

Рис. 2. Граф переходов при $n = 1$

Семейство индексов состояний $N_+ = \{1, 3, 4\}$, в которых $z_i = 1$. В результате преобразований Лапласа получаем:

$$\tilde{P}_{11}(s) = \frac{1}{s}\left[1 - f_1(s)\right];$$

$$\tilde{P}_{13}(s) = \frac{1}{s} P_1 f_1(s) g_2(s);$$

$$\tilde{P}_{14}(s) = \frac{1}{s}(1 - P_1) f_1(s).$$

Вышеприведенное семейство формул, отражающих индексы состояний N_+, будет зависеть от имеющегося ресурса и ресурсоёмкости восстановительных работ.

В результате применения математической модели с применением преобразования Лапласа получаем результирующее выражение:

$$\tilde{\varphi}(s) = \sum_{i \in N_+} \tilde{P}_{1i}(s) = \frac{1}{s}\left[1 - f_1(s)\right] + \frac{1}{s} P_1 f_1(s) g_2(s) + \frac{1}{s}(1 - P_1) f_1(s).$$

Преобразовав, получаем: $\tilde{\varphi}(s) = \frac{1}{s} + \frac{1}{s} P_1 f_1(s) g_2(s) - \frac{1}{s} P_1 f_1(s)$.

Применяя обратное преобразование Лапласа, получаем:

$$\varphi(t) = 1 - P_1 F_1(t) + P_1 \int_0^t F_1(t - \tau) g_2(\tau) d\tau;$$

$$\varphi(t) = 1 - P_1 F_1(t) + P_1 F_1(t) * g_2(t), \qquad (6)$$

где знак * означает операцию свертки двух функций. При моделировании принимается допущение, что неравенство (2) выполняется. На текущем этапе исследования граф переходов и семейство индексов состояний формируются вручную. Построение алгоритма, позволяющего автоматизировать процесс, находится за рамками настоящего исследования. При поиске решения следует учитывать условие неравенства (2).

5. Результаты моделирования. Результаты моделирования приведены на рисунках 3–5.

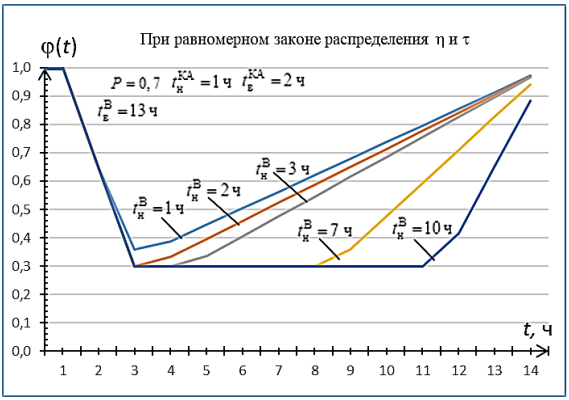

Рис. 3. Поведение функции живучести φ (*t*) при изменении нижней границы времени восстановления $t_н^В$ функциональности Элемента

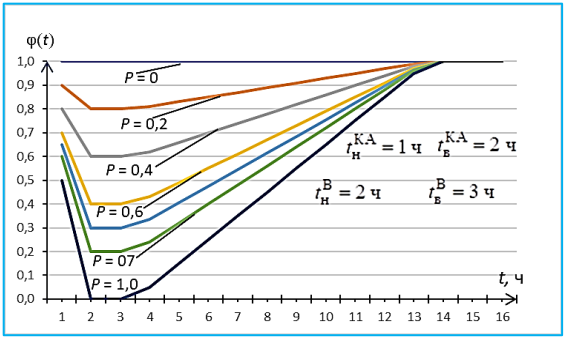

Рис. 4. Функция живучести φ (*t*) при изменении вероятности поражения Элемента

Первые два результата получены при аппроксимации функций распределения случайных времен до воздействия противника и восстановления функционала Элемента равномерным законом распределения. Анализ результатов позволяет утверждать, что вид функции φ(*t*), в том числе и минимальное ее значение φ_m и время t_m зависят от вероятности поражения *P* (защищенности) Элемента (рисунок 4), характеристик КА, а также от производственной возможности системы восстановления функционала.

На рисунке 5 приведены результаты построения функции живучести при аппроксимации функций распределения случайных времен до воздействия противника и восстановления функционала Элемента экспоненциальным законом распределения.

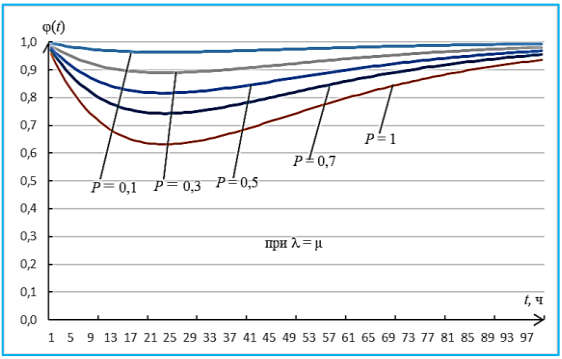

Рис. 5. Поведение функции живучести φ (*t*) при изменении вероятности поражения Элемента

Применение этого закона распределения позволяет получить более простую математическую модель в виде аналитической зависимости. При некоторых условиях такая замена приводит к незначительной погрешности и может быть вполне допустима. Исследование величины такой погрешности находится на стадии завершения, результаты будут приведены в другой публикации.

Из полученного соотношения (6) интуитивно выведены, на качественном уровне, следующие предельные свойства функции живучести:

1) $\varphi(0) = 1$, значение функции живучести в начальный момент времени равно 1;

2) $\lim_{t\to\infty}\varphi(t)=1$, в отсутствии КА $F_1(t) = 0$, следовательно, предельное значение функции живучести Элемента в этом случае равно единице;

3) $\varphi(t, P_i = 0) = 1$, если вероятности поражения Элемента при КА равны нулю (это может быть в случае, если средства поражения противника слабы либо рубежи защиты Элемента сильны) значение функция живучести Элемента также равно единице. Перечисленные утверждения не противоречат логике вещей.

6. Заключение. Таким образом, результаты исследований позволяют утверждать, что для аудиторского оценивания

функциональной живучести элементов ИИ и построения соответствующей программы аудита возможно применение известных методов теории полумарковских процессов.

Исследование предмета теории полумарковских процессов показывает, что для решения поставленной задачи существенным является модификация полумарковской модели с целью учета ограничений на ресурс, который поддерживает реальный процесс функционирования Элемента в условиях КА.

Разработанный подход целесообразно применять при относительно небольшом количестве КА, как показал эксперимент, не больше трех. При увеличении числа КА выражения для функции живучести становятся весьма громоздкими и трудно интерпретируемыми, поэтому требуется автоматизация процесса моделирования.

Предлагаемый подход может быть применен для оценивания достоверности статистических моделей на выборках не больше трех и формирования заключения, по аналогии, о достоверности статистических моделей для бóльших n, что важно для практики.

Литература

1. Отчет о сетевой безопасности и доступности в 2020 году. URL: https://qrator.net/presentations/2021/QratorLabs_Network_Security_Availability_in_2020_RU.pdf. (дата обращения: 01.03.2023).
2. Data Breach Investigations Report. Available at: https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf. (accessed 01.03.2023).
3. Attacks on Russian companies in the 3rd quarter of 2022. Rostelecom-Solar Report. Available at: https://ict.moscow/research/ataki-na-rossiiskie-kompanii-v-iii-kvartale-2022-goda/?amp&amp&amp. (accessed 01.03.2023).
4. National Institute of Standards and Technology Special Publication 800-53A, Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans. Available at: https://www.nist.gov/publications/guide-assessing-security-controls-federal-information-systems-and-organizations. (accessed 01.03.2023).
5. Авдуевский В.С. Надежность и эффективность в технике. Справочник. Проектный анализ надежности. – М.: Машиностроение, 1989. Т. 5. 376 с.
6. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности. М.: Наука, 1965. 524 с.
7. Кульба В.В., Сомов С.К., Шелков А.Б. Анализ влияния использования информационной избыточности на показатели надежности распределенных информационных систем // Надежность. 2022. № 1. С. 4–12. DOI: 10.21683/1729-2646-2022-22-1-4-12.
8. Карантаев В.Г., Карпенко В.И. Применение комбинированных методов оценки надежности ИЭУ РЗА ЦПС с учетом фактора влияния кибератак // Методические вопросы исследования надежности больших систем энергетики: Материалы 94-го заседания Международного научного семинара (г. Алушта, 19–23 сентября 2022 г.) // Иркутск: Федеральное государственное бюджетное

учреждение науки Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук, 2022. С. 524–533.
9. Ефремов В.А., Мищенко В.И., Мищенко И.В. Полумарковская модель процесса функционирования средств измерений // Измерение. Мониторинг. Управление. Контроль. 2022. № 3(41). С. 29–38. DOI: 10.21685/2307-5538-2022-3-3.
10. Зеленцов Б.П. Модель системы мониторинга объекта при недостоверном контроле // Надежность. 2020. Т. 20. № 4. С. 3–12. DOI: 10.21683/1729-2646-2020-20-4-3-12.
11. Obzherin Yu.E., Sidorov S.M., Fedorenko S.N. Analysis of the time reserve influence on the technological cell productivity // MATEC Web of Conferences. 2017. vol. 129. p. 03009. DOI: 10.1051/matecconf/201712903009.
12. Xu X., Bishop M., Oikarinen D.G., Hao C. Application and modeling of battery energy storage in power systems // CSEE Journal of Power and Energy Systems. vol. 2. № 3. 2016. pp. 82–90.
13. Привалов А.А., Бекбаев Г.А. Оценка устойчивости телекоммуникационной сети железнодорожной станции на основе схемы функциональной целостности // 72-я Всероссийская научно-техническая конференция, посвященная Дню радио: Труды конференции (г. Санкт-Петербург, 20–28 апреля 2017 г.). СПб: Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина). 2017. С. 293–295.
14. Dorofeev A.V., Markov A.S. Conducting Cyber Exercises Based on the Information Security Threat Model // CEUR Workshop Proceedings. 2021. pp. 1–10.
15. 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.
16. Недосекин А.О., Виноградов В.В. Оценка динамическом функциональной живучести технической системы в условиях неопределенности // Мягкие измерения и вычисления. 2017. № 1(1). С. 58–64.
17. 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.
18. Гавдан Г.П., Иваненко В.Г., Рыбалко Э.П., Рыбалко Д.П. Устойчивость функционирования объектов критической информационной инфраструктуры // Безопасность информационных технологий. 2022. Т. 29. № 4. С. 53–66. DOI: 10.26583/bit.2022.4.05.
19. Антонов С.Г., Анциферов И.И., Климов С.М. Методика инструментально-расчетной оценки устойчивости объектов критической информационной инфраструктуры при информационно-технических воздействиях. Надежность. 2020. Т. 20(4). pp. 35–41. DOI: 10.21683/1729-2646-2020- 20-4-35-41.
20. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52–61. DOI: 10.24411/2409-5419-2018-10041.
21. Privalov A., Titov D., Kotenko I., Saenko I., Evglevskaya N. Evaluating the functioning quality of data transmission networks in the context of cyberattacks // Energies. 2021. vol. 14. no. 16. DOI: 10.3390/en14164755.
22. Милашевский А.В., Мякотин А.В., Привалов А.А., Чеботарев В.И. Факторы, влияющие на функциональную целостность и устойчивость функционирования подвижного узла связи специального назначения // Известия Тульского государственного университета. Технические науки. 2020. № 11. С. 339–344.

23. Краснов А.Е., Мосолов А.С., Феоктистова Н.А. Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности // Безопасность информационных технологий. 2021. Т. 28. № 1. С. 106–120. DOI: 10.26583/bit.2021.1.09.
24. Максимова Е.А., Садовникова Н.П. Оценка инфраструктурной устойчивости субъекта критической информационной инфраструктуры при деструктивных воздействиях // Известия ЮФУ. Технические науки. 2021. № 4(221). С. 155–165. DOI: 10.18522/2311-3103-2021-4-155-165.
25. Ледовских Т.В., Щербакова Е.Н. Требования к устойчивости сетей связи субъектов критической информационной инфраструктуры // Технологии информационного общества: Материалы XIII Международной отраслевой научно-технической конференции (г. Москва, 20–21 марта 2019 г.). М.: ООО «Издательский дом Медиа паблишер», 2019. С. 55–57.
26. Linkov I., Eisenberg D.A., Plourde K. Seager T.P., Allen J., Kott A. Resilience metrics for cyber systems. Environ Syst. Decis. 2013. vol. 33. pp. 471–476. DOI: 10.1007/s10669-013-9485-y.
27. Kott A., Linkov I. To Improve Cyber Resilience, Measure It. IEEE Computer. 2021. vol. 54. no. 2. p. 80–85.
28. Лившиц И.И. К вопросу управления уязвимостями в компонентах АСУТП // Автоматизация в промышленности. 2022. № 8. С. 12–16. DOI: 10.25728/avtprom.2022.08.02.
29. Grusho A.A., Grusho N.A., Zabezhailo M.I., Timonina E.E. Localization of the Root Cause of the Anomaly // Automatic Control and Computer Sciences. 2021. vol. 55. no. 8. pp. 978–983. DOI: 10.3103/S0146411621080137.
30. Тихонов В.И., Миронов М.А. Марковские процессы. М.: «Сов. радио», 1977. 488 с.
31. Вентцель Е.С. Теория вероятностей. Учеб. для вузов // М.: Высш. Шк., 2006. 575 с.
32. Voevodin V.A., Burenok D.S., Cherniaev V.S. Technique for Detecting Computer Attacks on a Wi-Fi Networks. Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). 2022. pp. 487–492. DOI: 10.1109/ElConRus54750.2022.9755703.
33. Voevodin V.A. Monte Carlo method for predicting the stability of the functioning of the informatization object in the conditions of massive computer attacks. International Conference «Marchuk Scientific Readings 2021» (MSR-2021) Journal of Physics: Conference Series. vol. 2099. 2021. DOI: 10.1088/1742-6596/2099/1/012070.
34. Макаренко С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. СПб: Издательство «Наукоемкие технологии», 2018. 122 с.
35. Макаренко С.И., Смирнов Г.Е. Методика обоснования тестовых информационно-технических воздействий, обеспечивающих рациональную полноту аудита защищенности объекта критической информационной инфраструктуры // Вопросы кибербезопасности. 2021. № 6(46). С. 12–25. DOI: 10.21681/2311-3456-2021-6-12-25.
36. Мищенко Д.А., Львов А.А., Никифоров А.А., Раад Джихад А.А., Светлов М.С. Полумарковская модель телекоммуникационной сети с динамическим управлением // Известия ЮФУ. Технические науки. 2021. № 5(222). С. 49–60. DOI: 10.18522/2311-3103-2021-5-49-60.
37. Песчанский А.И. Полумарковские модели профилактики ненадежной одноканальной системы обслуживания с потерями // ООО «Научно-издательский центр Инфра-М», 2022. 267 с. DOI: 10.12737/1870597.

38. Привалов А.А., Милашевский А.В. Подход к моделированию узла связи специального назначения, уязвимого к факторам деструктивного воздействия // Инновационная железная дорога. Новейшие и перспективные системы обеспечения движения поездов. Проблемы и решения: Сборник статей Международной научно-теоретической конференции (г. Санкт-Петербург, Петергоф, 18 мая 2021 г.). СПб, Петергоф: Военный институт (железнодорожных войск и военных сообщений), 2021. С. 308–315.
39. Yu S.-Z. Hidden Semi-Markov Models: Theory, Algorithms and Applications. Elsevier, 2015. 208 p.
40. Barbu V.S., Limnios N. Semi-Markov Chains and Hidden Semi-Markov Models toward Applications: their use in Reliability and DNA Analysis. Springer, 2008. 226 p.
41. Hoek J., Elliott R.J. Introduction to Hidden Semi-Markov Models. Cambridge University Press, 2018. 185 p.
42. Grabski F. Semi-Markov Processes: Applications in System Reliability and Maintenance. Elsevier, 2015. 255 p.
43. Obzherin Yu.E., Boyko E.G. Semi-Markov Models: Control of Restorable Systems with Latent Failures. Elsevier, Academic Press, 2015. 212 p.

Воеводин Владислав Александрович — канд. техн. наук, доцент кафедры, кафедра информационной безопасности, Национальный исследовательский университет «Московский институт электронной техники». Область научных интересов: модели, методы и средства обеспечения аудита состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, модели и методы оценки защищенности информации, в том числе в интересах страхования информационных рисков, методы оценки эффективности систем (комплексов) мер обеспечения информационной безопасности. Число научных публикаций — 50. vva541@mail.ru; улица Солнечная Аллея, 901, 124575, Москва, Россия; р.т.: +7(985)787-1344.

DOI 10.15622/ia.22.3.8

V. VOEVODIN

A MODEL FOR ASSESSING THE FUNCTIONAL STABILITY OF INFORMATION INFRASTRUCTURE ELEMENTS FOR CONDITIONS OF EXPOSURE TO MULTIPLE COMPUTER ATTACKS

Voevodin V. **A Model for Assessing the Functional Stability of Information Infrastructure Elements for Conditions of Exposure to Multiple Computer Attacks.**

Abstract. Information is given about a new approach to the application of methods of the theory of semi-Markov processes to solve the applied problem of assessing the functional stability of elements that make up the information infrastructure, functioning under the influence of multiple computer attacks. The task of assessing functional stability is reduced to the task of finding the survivability function of the element under study and determining its extreme values. The relevance of the study is substantiated. The rationale is based on the assumption that quantitative methods of studying the stability of technical systems, which operate on the theory of reliability, cannot always be used to assess survivability. The concepts of «stability» and «computer attack» are being clarified. Verbal and formal statements of research tasks are formulated. The novelty of the results obtained lies in the application of well-known methods to solve a practically significant problem in a new formulation, taking into account the limitations on the resource allocated to maintain the survivability of the element under study, provided that arbitrary distribution laws are adopted for the random times of the implementation of computer attacks and the recovery times of the functional element. Recommendations on the formation of initial data, the content of the enlarged stages of modeling and a test case to demonstrate the performance of the model are given. The results of the test simulation are presented in the form of graphs of the survivability function. The resulting application can be used in practice to construct a survivability function when implementing up to three computer attacks, as well as a tool for evaluating the reliability of analogous statistical models. The limitation is explained by a progressive increase in the dimension of the analytical model and a decrease in the possibility of its meaningful interpretation.

Keywords: information infrastructure, information infrastructure element, functional stability, survivability function, computer attack, information security audit, semi-Markov processes, threats to information security.

References

1. Otchet o setevoj bezopasnosti i dostupnosti v 2020 godu. [Report on Netshhork security and Availability in 2020]. Available at: https://jarator.net/presentations/2021/JaratorLabs_Netshhork_Security_Availability_in_2020_RU.pdf. (accessed 01.03.2023). (In Russ.).
2. Data Breach Investigations Report. Available at: https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf. (accessed 01.03.2023).
3. Attacks on Russian companies in the 3rd quarter of 2022. Rostelecom-Solar Report. Available at: https://ict.moscow/research/ataki-na-rossiiskie-kompanii-v-iii-kvartale-2022-goda/?amp&amp&amp. (accessed 01.03.2023).
4. National Institute of Standards and Technology Special Publication 800-53A, Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans. Available at:

https://www.nist.gov/publications/guide-assessing-security-controls-federal-information-systems-and-organizations. (accessed 01.03.2023).
5. Авдуевский B.C. Nadezhnost' i jeffektivnost' v tehnike. Spravochnik. Proektnyj analiz nadezhnosti. [Reliability and efficiency in technology. Directory. Design reliability analysis]. Moscow: Mashinostroenie, 1989. 376 p. (In Russ.).
6. Gnedenko B.V., Beljaev Ju.K., Solov'ev A.D. Matematicheskie metody v teorii nadezhnosti [Mathematical Methods in Reliability Theory]. Moscow: Nauka, 1965. 524 p. (In Russ.).
7. Kul'ba V.V., Somov S.K., Shelkov A.B. [Analysis of the influence of the use of information redundancy on the reliability indicators of distributed information systems]. Nadezhnost' – Reliability. 2022. no. 1. pp. 4–12. DOI: 10.21683/1729-2646-2022-22-1-4-12. (In Russ.).
8. Karantaev V.G., Karpenko V.I. [The use of combined methods for assessing the reliability of the IED RPA CPS, taking into account the influence of cyber attacks] Metodicheskie voprosy issledovanija nadezhnosti bol'shih sistem jenergetiki: Materialy 94-go zasedanija Mezhdunarodnogo nauchnogo seminara [Methodological Issues of Researching the Reliability of Large Energy Systems: Proceedings of the 94th meeting of the International Scientific Seminar] Irkutsk: Federal'noe gosudarstvennoe bjudzhetnoe uchrezhdenie nauki Institut sistem jenergetiki im. L.A. Melent'eva Sibirskogo otdelenija Rossijskoj akademii nauk, 2022. pp. 524–533. (In Russ.).
9. Efremov V.A. Mishhenko V.I., Mishhenko I.V. [Semi-Markov model of the process of functioning of measuring instruments]. Izmerenie. Monitoring. Upravlenie. Kontrol' – Measurement. Monitoring. Control. 2022. № 3(41). pp. 29–38. DOI: 10.21685/2307-5538-2022-3-3. (In Russ.).
10. Zelencov B.P. [Model of the monitoring system of an object with unreliable control]. Nadezhnost' – Reliability. 2020. T. 20. № 4. p. 3–12. DOI: 10.21683/1729-2646-2020-20-4-3-12. (In Russ.).
11. Obzherin Ju.E., Sidorov S.M., Fedorenko S.N. Analysis of the time reserve influence on the technological cell productivity. MATEC Web of Conferences. 2017. vol. 129. p. 03009. DOI: 10.1051/matecconf/201712903009.
12. Xu X., Bishop M., Oikarinen D.G., Hao C. Application and modeling of battery energy storage in power systems. CSEE Journal of Power and Energy Systems. vol. 2. № 3. 2016. pp. 82–90.
13. Privalov A.A., Bekbaev G.A. [Assessment of the stability of the telecommunications network of a railway station based on the scheme of functional integrity] 72-ja Vserossijskaja nauchno-tehnicheskaja konferencija, posvjashhennaja Dnju radio: Trudy konferencii [72nd All-Russian Scientific and Technical Conference dedicated to Radio Day], Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj jelektrotehnicheskij universitet «LJeTI» im. V.I. Ul'janova (Lenina), 2017. pp. 293–295.
14. Dorofeev A.V., Markov A.S. Conducting Cyber Exercises Based on the Information Security Threat Model. CEUR Workshop Proceedings. 2021. pp. 1–10.
15. Markov A.S., Cirlov V.L., Barabanov A.V. Metody ocenki nesootvetstvija sredstv zashhity informacii [Methods for assessing the inconsistency of information security tools]. Moscow: Radio i svjaz', 2012. 192 p.
16. Nedosekin A.O., Vinogradov V.V. [Assessment of the dynamic functional survivability of a technical system under conditions of uncertainty]. Mjagkie izmerenija i vychislenija – Soft measurements and calculations. 2017. № 1(1). pp. 58–64. (In Russ.).
17. Hohlachev E.N. Organizacija i tehnologii vyrabotki reshenij pri upravlenii sistemoj i vojskami svjazi. Chast' 2. Vyrabotka reshenij pri vosstanovlenii setej svjazi [Organization and technologies for making decisions in the management of the system

and signal troops. Part 2. Development of solutions for the restoration of communication networks]. Moscow: VA RVSN, 2009. 241 p. (In Russ.).
18. Gavdan G.P., Ivanenko V.G., Rybalko Je.P., Rybalko D.P. [Sustainability of functioning of objects of critical information infrastructure] Bezopasnost' informacionnyh tehnologij – Information technology security. 2022. vol. 29. no. 4. pp. 53–66. DOI: 10.26583/bit.2022.4.05. (In Russ.).
19. Antonov S.G., Anciferov I.I., Klimov S.M. [Methodology for instrumental-calculative assessment of the stability of critical information infrastructure objects under information and technical impacts]. Nadezhnost' – Reliability. 2020. 20(4). pp. 35–41. DOI: 10.21683/1729-2646-2020- 20-4-35-41. (In Russ.).
20. Zaharchenko R.I., Korolev I.D. [Methodology for assessing the sustainability of the functioning of objects of critical information infrastructure operating in cyberspace]. Naukoemkie tehnologii v kosmicheskih issledovanijah Zemli – Science-intensive technologies in space exploration of the Earth. 2018. vol. 10. no. 2. pp. 52–61. DOI: 10.21683/1729-2646-2020- 20-4-35-41 10.24411/2409-5419-2018-10041. (In Russ.).
21. Privalov A., Titov D., Kotenko I., Saenko I., Evglevskaya N. Evaluating the functioning quality of data transmission networks in the context of cyberattacks. Energies. 2021. vol. 14. no. 16. DOI: 10.3390/en14164755.
22. Milashevskij A.V., Mjakotin A.V., Privalov A.A., Chebotarev V.I. [Factors affecting the functional integrity and stability of the operation of a special-purpose mobile communication center]. Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki – News of the Tula State University. Technical science. 2020. no. 11. pp. 339–344. (In Russ.).
23. Krasnov A.E., Mosolov A.S., Feoktistova N.A. [Assessing the resilience of critical information infrastructures to information security threats] Bezopasnost' informacionnyh tehnologij – Information technology security. 2021. vol. 28. no. 1. pp. 106–120. DOI: 10.26583/bit.2021.1.09. (In Russ.).
24. Maksimova E.A., Sadovnikova N.P. [Assessment of infrastructure stability of the subject of critical information infrastructure under destructive impacts]. Izvestija JuFU. Tehnicheskie nauki. – Izvestiya SFedU. Technical science. 2021. vol. 4(221). pp. 155–165. DOI: 10.18522/2311-3103-2021-4-155-165. (In Russ.).
25. Ledovskih T.V., Shherbakova E.N. [Requirements for the stability of communication networks of subjects of critical information infrastructure] Tehnologii informacionnogo obshhestva: Materialy HIII Mezhdunarodnoj otraslevoj nauchno-tehnicheskoj konferencii [Technologies of the Information Society: Proceedings of the XIII International Industry Scientific and Technical Conference]. Moscow: OOO «Izdatel'skij dom Media pablisher», 2019. pp. 55–57. (In Russ.).
26. Linkov I., Eisenberg D.A., Plourde K. Seager T.P., Allen J., Kott A. Resilience metrics for cyber systems. Environ Syst. Decis. 2013. vol. 33. pp. 471–476. DOI: 10.1007/s10669-013-9485-y.
27. Kott A., Linkov I. To Improve Cyber Resilience, Measure It. IEEE Computer. 2021. vol. 54. no. 2. p. 80–85.
28. Livshic, I.I. [On the Issue of Vulnerability Management in APCS Components]. Avtomatizacija v promyshlennosti – Automation in industry. 2022. № 8. pp. 12–16. DOI: 10.25728/avtprom.2022.08.02. (In Russ.).
29. Grusho A.A., Grusho N.A., Zabezhailo M.I., Timonina E.E. Localization of the Root Cause of the Anomaly. Automatic Control and Computer Sciences. 2021. vol. 55. no. 8. pp. 978–983. DOI: 10.3103/S0146411621080137.
30. Tihonov V.I., Mironov M.A. Markovskie process [Markov processes]. Moscow, «Sov. radio», 1977. 488 p. (In Russ.).
31. Ventcel' E.S. Teorija verojatnostej. Ucheb. dlja vuzov [Probability Theory. Textbook for universities]. Moscow, Vyssh. Shk., 2006. 575 p. (In Russ.).

32. Voevodin V.A., Burenok D.S., Cherniaev V.S. Technique for Detecting Computer Attacks on a Wi-Fi Networks. Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). 2022. pp. 487–492. DOI: 10.1109/ElConRus54750.2022.9755703.
33. Voevodin V.A. Monte Carlo method for predicting the stability of the functioning of the informatization object in the conditions of massive computer attacks. International Conference «Marchuk Scientific Readings 2021» (MSR-2021) Journal of Physics: Conference Series. vol. 2099. 2021. DOI: 10.1088/1742-6596/2099/1/012070.
34. Makarenko, S.I. Audit bezopasnosti kriticheskoj infrastruktury specialnymi informacionnymi vozdejstvijami [Security audit of critical infrastructure by special information impacts]. Sankt-Peterburg: Izdatel'stvo «Naukoemkie tehnologii», 2018. 122 p. (In Russ.).
35. Makarenko S.I., Smirnov G.E. [Methodology for substantiating test information and technical impacts that ensure the rational completeness of the security audit of a critical information infrastructure object]. Voprosy kiberbezopasnosti – Cybersecurity Issues. 2021. № 6(46). pp. 12–25. DOI: 10.21681/2311-3456-2021-6-12-25. (In Russ.).
36. Mishhenko D.A., L'vov A.A., Nikiforov A.A., Raad Dzhihad A.A., Svetlov M.S. [Semi-Markov model of a telecommunications network with dynamic control]. Izvestija JuFU. Tehnicheskie nauki – Izvestiya SFedU. Technical science. 2021. № 5(222). pp. 49-60. DOI: 10.18522/2311-3103-2021-5-49-60. (In Russ.).
37. Peschanskij A.I. Polumarkovskie modeli profilaktiki nenadezhnoj odnokanalnoj sistemy obsluzhivanija s poterjami [Semi-Markov prevention models for an unreliable single-channel queuing system with losses]. OOO «Nauchno-izdatel'skij centr Infra-M», 2022. 267 p. DOI: 10.12737/1870597. (In Russ.).
38. Privalov A.A., Milashevskij A.V. [An Approach to Modeling a Special-Purpose Communication Center Vulnerable to Destructive Impact Factors] Innovacionnaja zheleznaja doroga. Novejshie i perspektivnye sistemy obespechenija dvizhenija poezdov. problemy i reshenija: Sbornik statej Mezhdunarodnoj nauchno-teoreticheskoj konferencii [Innovative railway. The latest and promising systems for ensuring the movement of trains. Problems and Solutions: Collection of articles of the International Scientific and Theoretical Conference]. Sankt-Peterburg, Petergof: Voenyj institut (Zheleznodorozhnyh vojsk i voennyh soobshhenij), 2021. pp. 308–315. (In Russ.).
39. Yu S.-Z. Hidden Semi-Markov Models: Theory, Algorithms and Applications. Elsevier, 2015. 208 p.
40. Barbu V.S., Limnios N. Semi-Markov Chains and Hidden Semi-Markov Models toward Applications: their use in Reliability and DNA Analysis. Springer, 2008. 226 p.
41. Hoek J., Elliott R.J. Introduction to Hidden Semi-Markov Models. Cambridge University Press, 2018. 185 p.
42. Grabski F. Semi-Markov Processes: Applications in System Reliability and Maintenance. Elsevier, 2015. 255 p.
43. Obzherin Yu.E., Boyko E.G. Semi-Markov Models: Control of Restorable Systems with Latent Failures. Elsevier, Academic Press, 2015. 212 p.

Voevodin Vladislav — Ph.D., Associate professor of the department, Department of information security, National Research University of Electronic Technology. Research interests: models, methods and means of auditing the condition of an object under the influence of threats to its information security, models and methods for assessing the security of information, including in the interests of information risk insurance, methods for evaluating the effectiveness of systems (complexes) measures to ensure information security. The number of publications — 50. vva541@mail.ru; 901, Sunny Alley St., 124575, Moscow-Zelenograd, Russia; office phone: +7(985)787-1344.