МЕТОДИКА ОЦЕНИВАНИЯ ИНФОРМАЦИОННОЙ УСТОЙЧИВОСТИ ГЕТЕРОГЕННОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

Коноваленко С.А.[1]

Цель исследования: *определение уточненного семантического значения, показателя и критерия оценивания информационной устойчивости процесса функционирования гетерогенной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также формирование на их основе целенаправленной последовательности действий для получения количественной оценки рассматриваемого аспекта устойчивости.*

Метод исследования: *системный анализ, системно-динамическое моделирование с использованием алгебраических выражений и логических условий.*

Результаты исследования: *определена необходимость разработки научно-методического аппарата оценивания информационной устойчивости процесса функционирования гетерогенной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на этапе ее эксплуатации в условиях деструктивных воздействий, направленных на нарушение ее процесса функционирования и доступности. Проведен анализ понятийного аппарата и выявлена терминологическая нечеткость в исследуемой предметной области. Сформировано уточненное семантическое значение, показатель и критерий оценивания информационной устойчивости процесса функционирования рассматриваемого объекта в заданных условиях эксплуатации. На основе представления заданного объекта оценивания в виде кибернетической системы и системно-динамической модели разработана система ключевых показателей и целенаправленная последовательность действий для получения количественной оценки текущего уровня рассматриваемого аспекта устойчивости. Предложены направления развития разработанного научно-методического аппарата оценивания информационной устойчивости процесса функционирования рассматриваемого объекта.*

Научная новизна *заключается в предоставлении теоретически обоснованного формализованного подхода к оцениванию информационной устойчивости процесса функционирования гетерогенной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, позволяющего, в отличии от известных, сформировать научно-технологический задел для получения комплексной оценки устойчивости заданного объекта и реализации предлагаемых научно-технических решение на практике.*

Ключевые слова: *кибернетическая система, системно-динамическая модель, скорость изменения информационного ресурса, уязвимость, компьютерная атака, процедуры функционально-параметрического управления, нарушение процесса функционирования, нарушение доступности.*

DOI: 10.21681/2311-3456-2023-6-67-80

Введение

В настоящее время обеспечение информационной безопасности (ИБ) объектов критической информационной инфраструктуры (КИИ) достигается путем эффективного функционирования гетерогенной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГетСОПКА) [1-3]. При этом, процесс функционирования (ПФ) объектов КИИ и ГетСОПКА, как средства обеспечения их безопасного применения, осуществляется в условиях [2, 3]:

— физических воздействий естественно-природных факторов окружающей среды, независимых от человека;

1 Коноваленко Сергей Александрович, кандидат технических наук, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: konovalenko_rcf@mail.ru

— неумышленных воздействий, вызванных ошибками или халатностью деятельности человека;
— умышленных воздействий, вызванных действиями со стороны потенциального злоумышленника, в условиях вооруженного или информационного конфликта.

Указанные условия эксплуатации объектов КИИ и ГетСОПКА, имея естественную или искусственную природу происхождения, проявляются в виде деструктивных преднамеренных (ДПВ) или непреднамеренных (ДНПВ) воздействий, оказывающих негативное влияние на ПФ и доступность рассматриваемых объектов, тем самым переводя их в неустойчивое состояние, в котором они не обеспечивают решение поставленных перед ними задач [2-4]. В свою очередь, для компенсации негативных последствий ДПВ и ДНПВ, направленных на нарушение ПФ и доступности объектов КИИ, в структуре ГетСОПКА выделены источники событий ИБ (ИСИБ), образующие подсистему ИСИБ (ПИСИБ), и специализированные средства (СС), образующие центральную подсистему сбора, хранения и корреляции событий ИБ (ЦПСХКСИБ), которые в общем реализуют набор определенных функций по контролю состояния защищенности объектов КИИ, по сбору, хранению и анализу событий ИБ (СИБ) с целью обнаружения инцидентов ИБ (ИИБ) на объектах КИИ и принятия решений по ликвидации их последствий [4, 5]. Кроме того, наряду с ПИСИБ и ЦПСХКСИБ, в структуре ГетСОПКА не выделена отдельная подсистема централизованного управления ПФ ИСИБ (СС) на этапе их эксплуатации в условиях ДПВ и ДНПВ, направленных на нарушение их ПФ и доступности, но решение рассматриваемой задачи осуществляется специалистами по ИБ в «ручном» режиме при отсутствии реализованных на практике комплексных технических решений, способных обеспечить автоматизацию рассматриваемого процесса, что свидетельствует о недостаточном уровне эффективности ПФ данного объекта в выделенных условиях эксплуатации [4, 5]. Стоит заметить, что вышеуказанная проблемная ситуация в практике применения ГетСОПКА обусловила необходимость проведения всестороннего анализа теоретических основ в заданной предметной области, в результате которого установлено, что необходимо разработать новый научно-методический аппарат функционально-параметрического управления (ФПУ) ПФ ИСИБ (СС) с учетом особенностей их построения, режимов функционирования (РжФ) и выделенных условий эксплуатации [4]. При этом, разработка указанного научно-методического аппарата должна включать последовательный синтез таких процедур, как адаптивный контроль состояния ПФ и оценивание информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в заданных режимах и условиях функционирования, а также синтез и реализация информационно-технического решения (ИТР) на ФПУ ее ПФ. Учитывая вышеуказанное, а также, что в работах [6-8] был разработан научно-методический аппарат адаптивного контроля состояния ПФ ГетСОПКА в условиях ДПВ и ДНПВ, направленных на нарушение ее ПФ и доступности, в данной работе решается актуальная научно-техническая задача разработки научно-методического аппарата оценивания информационной устойчивости ПФ рассматриваемого объекта в выделенных условиях эксплуатации, что в общем может стать основой для построения подсистемы централизованного ФПУ (ПФПУ) ПФ рассматриваемого объекта [4].

Анализ теоретических основ реализации процедуры оценивания информационной устойчивости ПФ ГетСОПКА

Практика реализации процедуры оценивания информационной устойчивости ПФ сложных технических систем (СТС), к которым относится ГетСОПКА, свидетельствует о том, что в настоящее время отсутствует единый структурированный подход к пониманию семантического значения и к определению показателей рассматриваемого аспекта устойчивости [9-11].

В существующих исследованиях под информационной устойчивостью ПФ СТС понимают способность СТС в динамике информационного конфликта своевременно, достоверно и скрытно реализовывать информационный обмен (передавать данные) между своими структурными элементами и осуществлять управление ими с учетом деструктивных воздействий, направленных на нарушение ПФ элементов СТС [9, 10]. Анализируя существующую интерпретацию понятия «информационная устойчивость ПФ СТС», выделим его терминологическую нечеткость:

1. Полный цикл ПФ любого структурного элемента СТС представляется в виде последовательного выполнения определенных операций, завершающей из которых является операция передачи результатов своего функционирования в адрес очередного структурного элемента СТС [12]. Свойства, в частности, своевременность, достоверность и скрытность, которые определяют качество операции передачи данных между структурными элементами системы и, как следствие, поведение СТС в целом, относятся к группе функциональных (операционных) свойств [12]. Указанное является

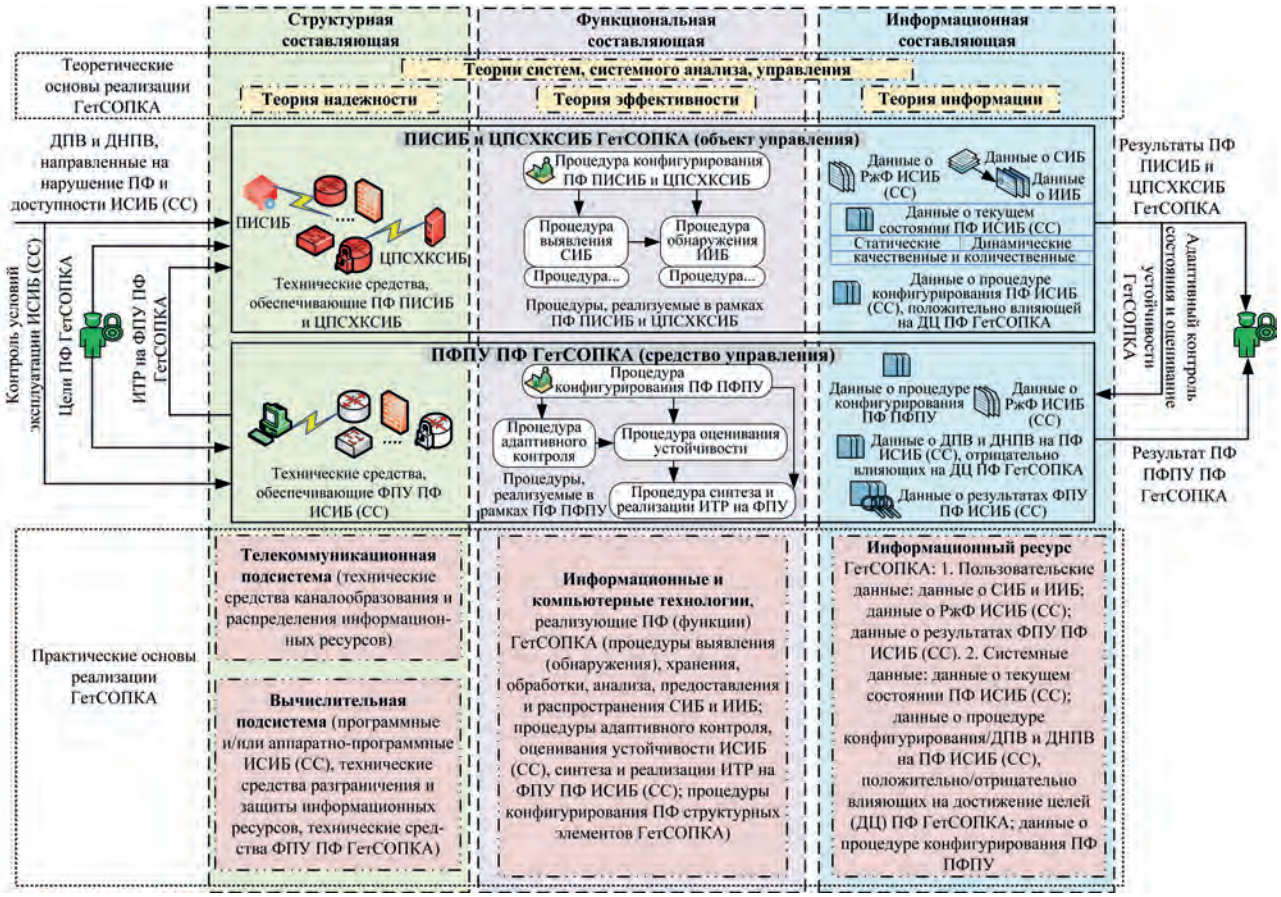

Рис. 1. Представление ГетСОПКА в виде кибернетической системы

свидетельством подмены понятий информационной и функциональной устойчивости ПФ СТС.

2. Оценивание информационной устойчивости ПФ СТС по степени управляемости структурными элементами СТС также не может в полной мере претендовать на адекватное решение так, как оба свойства «устойчивость» и «управляемость» одновременно являются общесистемными свойствами, определяющими принципиально разные аспекты качества ПФ СТС [12].

С учетом проведенного анализа понятийного аппарата и выявленной терминологической нечеткости в исследуемой предметной области возникает необходимость в уточнении семантического значения рассматриваемого понятия, а также определении его показателя и критерия оценивания с учетом особенностей построения ГетСОПКА, ее РжФ и условий эксплуатации.

Для определения семантического значения и показателя информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в заданном РжФ в условиях ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ИСИБ (СС), представим рассматриваемый объект в виде кибернетической системы (рис. 1) [9, 12, 13].

На рис. 1 ГетСОПКА описывается с трех точек зрения:

1. Структурная составляющая ГетСОПКА, представляющая собой совокупность разнотипных технических средств, с одной стороны входящих в состав телекоммуникационной или вычислительной подсистем рассматриваемой системы, а с другой стороны обеспечивающих реализацию ПФ объекта (ПИСИБ и ЦПСХКСИБ) и средства (ПФПУ) управления.

2. Функциональная составляющая ГетСОПКА, представляющая собой совокупность определенных процедур, выполняемых в рамках применяемых информационных и компьютерных технологий, реализующих ПФ объекта (ПИСИБ и ЦПСХКСИБ) и средства (ПФПУ) управления.

3. Информационная составляющая ГетСОПКА, представляющая собой совокупность пользовательских и системных данных, образующих информационный ресурс рассматриваемой системы, а также отражающих степень достижения целей и разнообразные свойства объекта (ПИСИБ и ЦПСХКСИБ) и средства (ПФПУ) управления на этапе их эксплуатации в штатном (ШРФ), усиленном (УРФ) или боевом (БРФ) РжФ при ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ИСИБ (СС).

Далее заметим, что в рамках данной работы рассмотрение структурной и функциональной составляющих ГетСОПКА и, как следствие, структурной и функциональной устойчивости ПФ рассматриваемого объекта в заданных режимах и условиях эксплуатации не предусмотрено.

Таким образом, основываясь на представлении рассматриваемого объекта в виде кибернетической системы (рис. 1), а в частности на его информационной составляющей, следует принять, что:

- под информационной устойчивостью ПФ ГетСОПКА понимается свойство ПФ ГетСОПКА, определяющее способность ПИСИБ и ЦПСХКСИБ на этапе их эксплуатации в произвольном (ζ) РжФ сохранять требуемый уровень информационного равновесия между факторами, положительно и отрицательно влияющими на достижение требуемого целевого эффекта (результата) их ПФ;
- показателем информационной устойчивости ПФ ГетСОПКА является скорость изменения набора (количества) данных (параметров) конфигурации (настройки) ПФ ПИСИБ и ЦПСХКСИБ в ζ-м РжФ при ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ИСИБ (СС) ($dY_{\zeta}^{\text{сопка/пдк}} / dt$);
- критерием оценивания информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в ζ-м РжФ при ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ИСИБ (СС), является:

$$dY_{\zeta}^{\text{сопка/пдк}} / dt \geq dY_{\zeta}^{\text{сопка/пдк/тр}} / dt \Big| \left(dY_{\zeta}^{\text{сопка/пдк/тр}} / dt\right) \geq 0, \ \zeta = \overline{1,3}, \quad (1)$$

где $dY_{\zeta}^{\text{сопка/пдк/тр}} / dt$ – допустимое значение скорости изменения набора (количества) данных (параметров) конфигурации (настройки) ПФ ПИСИБ и ЦПСХКСИБ в ζ-м РжФ, характеризующее требуемый уровень информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в условиях ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ИСИБ (СС);
$\zeta=1$, $\zeta=2$, $\zeta=3$ – соответственно ШРФ, УРФ, и БРФ ГетСОПКА.

Системно-динамическая модель ГетСОПКА

При оценивании информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в ζ-м РжФ при ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ИСИБ (СС), необходимо четко понимать особенности динамики ПФ рассматриваемого объекта и выделять множество факторов, положительно и отрицательно влияющих на достижение требуемого целевого эффекта (результата) его ПФ. В настоящее время наиболее адекватным методом, позволяющим обеспечить решение вышеуказанной задачи, является метод системно-динамического моделирования, которой направлен на изучение сложных динамических систем посредством исследования их состояния во времени в зависимости от особенностей построения их структурных элементов, взаимодействия между ними и влияния на них различного рода воздействий внешней среды и внутренних процессов [14, 15]. В основе метода системно-динамического моделирования находятся:

- системная потоковая диаграмма, строящаяся на основе типовых символов, представленных в табл. 1;
- система дифференциальных уравнений, которые позволяют рассчитать и представить в количественном выражении динамические изменения, происходящие в системе.

Далее на основе методологии системно-динамического моделирования рассмотрим ГетСОПКА как динамическую систему и представим ее с использованием системной потоковой диаграммы (рис. 2) [4, 14, 15].

Стоит еще раз отметить, что представление ГетСОПКА в виде кибернетической системы (рис. 1) и системно-динамической модели (рис. 2) возможно использовать не только для оценивания информационной устойчивости ПФ рассматриваемого объекта в заданных режимах и условиях эксплуатации, но и для оценивания ее структурной и функциональной устойчивости, порядок выполнения которого не приводится в данной работе в силу ранее введенного ограничения, связанного с рассмотрением только информационной составляющей ГетСОПКА.

С учетом системной потоковой диаграммы, описывающей системно-динамическую модель заданного объекта (рис. 2), а также особенностей его построения, как кибернетической системы (рис. 1), расчет текущего значения $dY_{\zeta}^{\text{сопка/пдк}} / dt$ выполним посредством аналитических методов (дифференциальных уравнений, алгебраических выражений и логических условий) при следующих общих допущениях [7, 16]:

- в состав ПИСИБ включено определенное ($\mu^{\text{писиб}}$) количество произвольных ($\rho^{\text{исиб}} = \overline{1, \mu^{\text{писиб}}}$) ИСИБ, а в состав ЦПСХКСИБ – определенное ($\varepsilon^{\text{цпсхксиб}}$) количество произвольных ($\varphi^{\text{сс}} = \overline{1, \varepsilon^{\text{цпсхксиб}}}$) СС;

Таблица 1.

Типовые символы, используемые в системной потоковой диаграмме

Графическое обозначение символа	Наименование символа	Назначение символа
	Уровень	Характеризует накопления внутри системы, возникающие в результате разности между входящими и исходящими потоками
	Темп	Обозначает скорость потока между уровнями в системе
	Потоковая связь	Соединяет уровни с уровнями, с истоками и стоками
	Информационная связь	Отражает информационные связи диаграммы
	Облако	Обозначает истоки и стоки потоков, которые не рассматриваются в модели
	Вспомогательная переменная	Специальный множитель (некоторая функция), влияющий на изменения моделируемых факторов

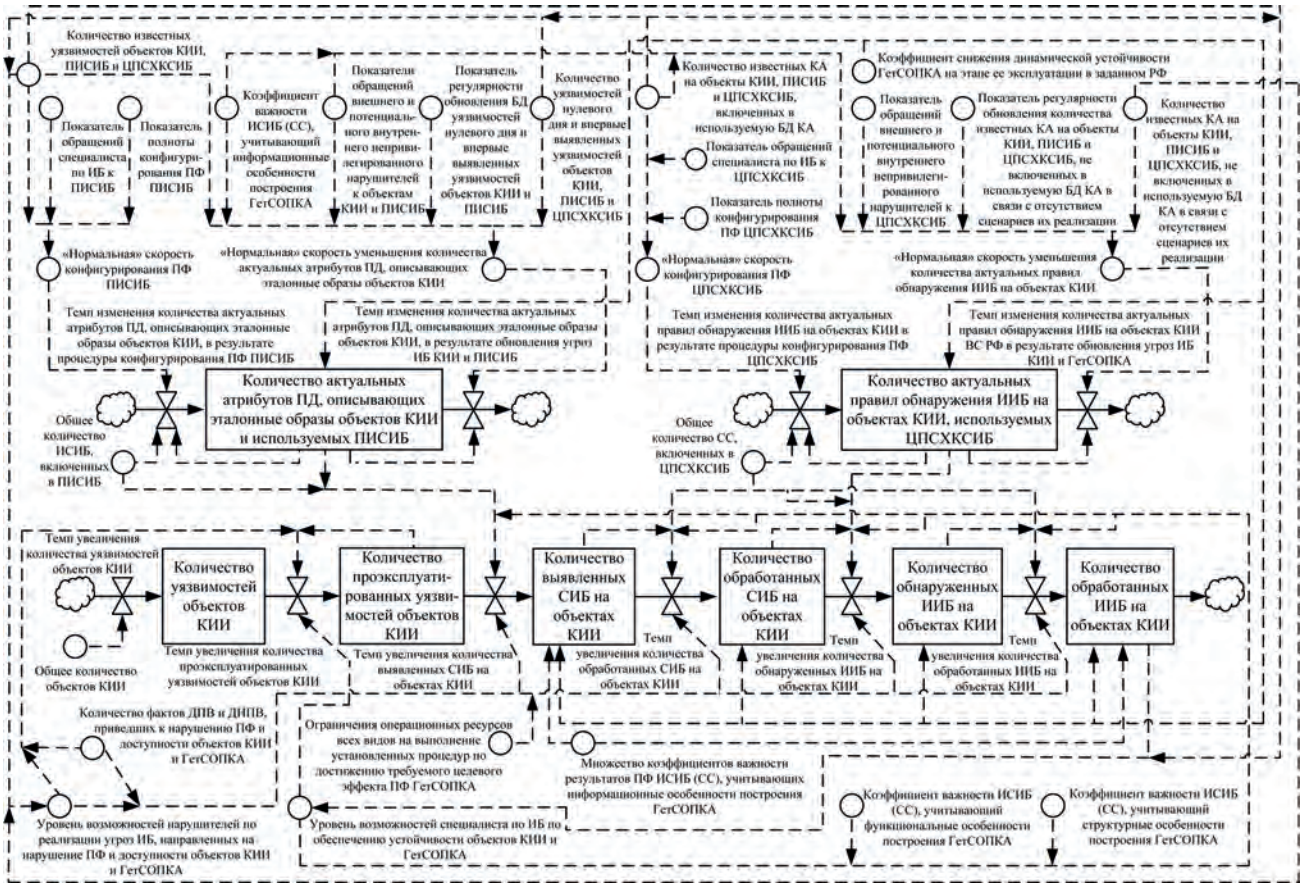

Рис. 2. Системная потоковая диаграмма, описывающая системно-динамическую модель ГетСОПКА

– ПФ $\rho^{\text{исиб}}$ направлен на выявление СИБ на определенных (контролируемых им) объектах КИИ и реализуется посредством контроля текущих значений атрибутов параметрических данных (ПД), описывающих эталонные образы соответствующих объектов;

– ПФ $\varphi^{\text{сс}}$ направлен на обнаружение ИИБ на определенных (контролируемых им) объектах КИИ и реализуется посредством автоматической обработки соответствующих СИБ, предоставляемых $\rho^{\text{исиб}}$, автоматического обнаружения ИИБ на основе применения предварительно заданных правил корреляции обработанных СИБ, а также с последующей обработкой обнаруженных ИИБ, в результате которой автоматически формируются соответствующие карточки ИИБ.

В дополнение к указанным общим допущениям для расчета текущего значения $dY_{\zeta}^{\text{сопка/пдк}} / dt$ введем следующие частные допущения:

1. Условно обозначим элементы системно-динамической модели ГетСОПКА (рис. 2), используемые при расчете текущего значения $dY_{\zeta}^{\text{сопка/пдк}} / dt$, в виде:

$Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$ – количество актуальных атрибутов ПД, описывающих эталонные образы определенных объектов КИИ и используемых $\rho^{\text{исио}}$ на этапе его эксплуатации в ζ-м РжФ (единица измерения (ед. изм.) – число актуальных атрибутов ПД);

$Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$ – количество актуальных правил обнаружения ИИБ на определенных объектах КИИ, используемых $\varphi^{\text{сс}}$ на этапе его эксплуатации в ζ-м РжФ (ед. изм. – число актуальных правил обнаружения ИИБ);

$IY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$, $BY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$ – соответственно темп изменения $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$ в результате процедуры конфигурирования ПФ $\rho^{\text{исиб}}$ и обновления угроз ИБ для определенных объектов КИИ и $\rho^{\text{исиб}}$ в ζ-м его РжФ (ед. изм. – число актуальных атрибутов ПД/ $\tau^{\text{оиу}}$, где $\tau^{\text{оиу}}$ – произвольный момент времени оценивания информационной устойчивости ПФ ГетСОПКА);

$DY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$, $PY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$ – соответственно темп изменения $Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$ в результате процедуры конфигурирования ПФ $\varphi^{\text{сс}}$ и обновления угроз ИБ для определенных объектов КИИ, $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – число актуальных правил обнаружения ИИБ/ $\tau^{\text{оиу}}$);

$\alpha_{\zeta}^{\rho^{\text{исио}}/\text{нск}}$, $\alpha_{\zeta}^{\varphi^{\text{сс}}/\text{нск}}$ – соответственно «нормальная» скорость конфигурирования ПФ $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ на этапе их эксплуатации в ζ-м РжФ (ед. изм. – соответственно число частей актуальных атрибутов ПД/ $\tau^{\text{оиу}}$ и число частей актуальных правил обнаружения ИИБ/ $\tau^{\text{оиу}}$);

$o_{\zeta}^{\rho^{\text{исио}}/\text{нсу}}$, $o_{\zeta}^{\varphi^{\text{сс}}/\text{нсу}}$ – соответственно «нормальная» скорость уменьшения $Y_{\zeta}^{\rho^{\text{исио}}/\text{пдк}}$ и $Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$ (ед. изм. – соответственно число частей актуальных атрибутов ПД/ $\tau^{\text{оиу}}$ и число частей актуальных правил обнаружения ИИБ/ $\tau^{\text{оиу}}$);

$\delta_{\zeta_{\text{окии}}^{\text{киу}}}^{\rho^{\text{исиб}}}$, $\psi_{\zeta_{\text{окии}}^{\text{ика}}}^{\varphi^{\text{сс}}}$ – соответственно общее количество известных уязвимостей и компьютерных атак (КА) на объекты КИИ, контролируемые $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – соответственно число известных уязвимостей и число известных КА, включенных в используемые базы данных (БД);

$\beta_{\zeta}^{\rho^{\text{исиб}}/\text{пос}}$, $\beta_{\zeta}^{\varphi^{\text{сс}}/\text{пос}}$ – соответственно показатель обращений специалиста по ИБ к $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – безразмерная величина);

$\nu_{\zeta}^{\rho^{\text{исиб}}/\text{ппк}}$, $\nu_{\zeta}^{\varphi^{\text{сс}}/\text{ппк}}$ – соответственно показатель полноты процедуры конфигурирования ПФ $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – безразмерная величина);

$k_{\zeta}^{\rho^{\text{исиб}}/\text{виу}}$, $k_{\zeta}^{\varphi^{\text{сс}}/\text{виу}}$ – соответственно коэффициент важности $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ, учитывающий информационные особенности построения ГетСОПКА, в частности объем передаваемого $\rho^{\text{исиб}}$ в адрес $\varphi^{\text{сс}}$ и принимаемого $\varphi^{\text{сс}}$ от $\rho^{\text{исиб}}$, $\rho^{\text{исиб}} = \overline{1,\ \mu^{\text{писиб}}}$, сетевого трафика с результатами (информацией о состоянии определенных объектов КИИ) его ПФ (ед. изм. – безразмерная величина) [16];

$\omega_{\zeta_{\text{окии}}^{\text{пон}}}^{\rho^{\text{исиб}}}$, $\omega_{\zeta}^{\rho^{\text{исиб}}/\text{пон}}$, $\omega_{\zeta}^{\varphi^{\text{сс}}/\text{пон}}$ – соответственно показатель обращений внешнего и потенциального внутреннего непривилегированного нарушителей к определенным (контролируемым $\rho^{\text{исиб}}$) объектам КИИ, к $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – безразмерная величина);

$\gamma_{\zeta}^{\rho^{\text{исиб}}/\text{ронву}}$ – показатель регулярности обновления БД уязвимостей нулевого дня и впервые выявленных уязвимостей определенных (контролируемых $\rho^{\text{исиб}}$) объектов КИИ и $\rho^{\text{исиб}}$ в ζ-м его РжФ (ед. изм. – безразмерная величина);

$\vartheta_{\zeta_{\text{окии}}^{\text{кнву}}}^{\rho^{\text{исиб}}}$, $\vartheta_{\zeta}^{\rho^{\text{исиб}}/\text{кнву}}$ – соответственно количество уязвимостей нулевого дня и впервые выявленных уязвимостей определенных (контролируемых $\rho^{\text{исиб}}$) объектов КИИ и $\rho^{\text{исиб}}$ в ζ-м его РжФ, которые могли быть проэксплуатированы внешним и потенциальным внутренним непривилегированным нарушителем за интервал времени $\left[\tau^{\text{оиу}} - 1, \tau^{\text{оиу}}\right]$ (ед. изм. – число уязвимостей нулевого дня и впервые выявленных/ $\tau^{\text{оиу}}$);

$k_{\zeta}^{\text{сопка/снду}}$ – коэффициент снижения динамической (информационной) устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в ζ-м РжФ, значение кото-

рого определяется на основе подходов, описанных в [16] (ед. изм. – безразмерная величина);

$\gamma_{\zeta}^{\varphi^{cc}/\text{роика}}$ – показатель регулярности обновления количество известных КА на определенные (контролируемые $\rho^{\text{исиб}}$) объекты КИИ, на $\rho^{\text{исиб}}$ (взаимодействующие с φ^{cc}) и на φ^{cc} в ζ-м их РжФ, не включенных в используемую БД КА в связи с отсутствием сценариев их реализации (ед. изм. – безразмерная величина);

$h_{\zeta_{\text{окии}}^{\text{ика}}}^{\rho^{\text{исиб}}}$, $h_{\zeta}^{\rho^{\text{исиб}}/\text{ика}}$, $h_{\zeta}^{\varphi^{cc}/\text{ика}}$ – соответственно количество известных КА на определенные (контролируемые $\rho^{\text{исиб}}$) объекты КИИ, на $\rho^{\text{исиб}}$ (взаимодействующие с φ^{cc}) и на φ^{cc} в ζ-м их РжФ, не включенных в используемую БД КА в связи с отсутствием сценариев их реализации и которые могли быть проведены внешним и потенциальным внутренним непривилегированным нарушителем за интервал времени $\left[\tau^{\text{оиу}}-1,\tau^{\text{оиу}}\right]$ (ед. изм. – число известных КА, не включенных в используемую БД КА/ $\tau^{\text{оиу}}$).

2. Специалист по ИБ на этапах подготовки и непосредственной эксплуатации ГетСОПКА, реализуя процедуру конфигурирования ПФ $\rho^{\text{исиб}}$ и φ^{cc}, под каждую отдельную (произвольную) известную уязвимость и КА на определенные объекты КИИ, принадлежащие $\delta_{\zeta_{\text{окии}}^{\text{киу}}}^{\rho^{\text{исиб}}}$ и $\psi_{\zeta_{\text{окии}}^{\text{ика}}}^{\varphi^{cc}}$, соответственно выделяет один актуальный атрибут ПД, принадлежащий $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$, и формирует одно актуальное правило обнаружения ИИБ, принадлежащее $Y_{\zeta}^{\varphi^{cc}/\text{пдк}}$.

3. Значения $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$ и $Y_{\zeta}^{\varphi^{cc}/\text{пдк}}$ могут соответствовать или быть меньше фактического (хранящегося в конфигурационных файлах $\rho^{\text{исиб}}$ и φ^{cc}) количества атрибутов ПД, описывающих эталонные образы определенных объектов КИИ, и правил обнаружения ИИБ на определенных объектах КИИ.

Методика оценивания информационной устойчивости ПФ ГетСОПКА

С учетом общих и частных допущений, введенных при построении системно-динамической модели ГетСОПКА (рис. 2), определим текущий уровень информационной устойчивости ПФ $\rho^{\text{исиб}}$ и φ^{cc} в $\tau^{\text{оиу}}$ момент времени на этапе их эксплуатации в ζ-м РжФ при ДПВ и ДНПВ, направленных на нарушение их ПФ и доступности, посредством расчета текущих значений скоростей изменения $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$ и $Y_{\zeta}^{\varphi^{cc}/\text{пдк}}$ (соответственно $dY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}/d\tau^{\text{оиу}}$ и $dY_{\zeta}^{\varphi^{cc}/\text{пдк}}/d\tau^{\text{оиу}}$) в виде:

$$
\begin{cases}
\dfrac{dY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}}{d\tau^{\text{оиу}}}=k_{\zeta}^{\text{сопка/снду}}\cdot\left(IY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}})-BY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}})\right);\\
IY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}})=\alpha_{\zeta}^{\rho^{\text{исиб}}/\text{нск}}(\tau^{\text{оиу}})\cdot Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}}-1);\\
BY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}})=o_{\zeta}^{\rho^{\text{исиб}}/\text{нсу}}(\tau^{\text{оиу}})\cdot Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}}-1);\\
\alpha_{\zeta}^{\rho^{\text{исиб}}/\text{нск}}(\tau^{\text{оиу}})=1+\beta_{\zeta}^{\rho^{\text{исиб}}/\text{пос}}(\tau^{\text{оиу}})\cdot\nu_{\zeta}^{\rho^{\text{исиб}}/\text{ппк}}(\tau^{\text{оиу}})\cdot\dfrac{\delta_{\zeta_{\text{окии}}^{\text{двкиу}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}})}{\delta_{\zeta_{\text{окии}}^{\text{киу}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}}-1)};\\
o_{\zeta}^{\rho^{\text{исиб}}/\text{нсу}}(\tau^{\text{оиу}})=k_{\zeta}^{\rho^{\text{исиб}}/\text{виу}}(\tau^{\text{оиу}})\cdot\dfrac{\left(\begin{array}{l}\omega_{\zeta_{\text{окии}}^{\text{пон}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}})\cdot\vartheta_{\zeta_{\text{окии}}^{\text{кнву}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}})+\\+\omega_{\zeta}^{\rho^{\text{исиб}}/\text{пон}}(\tau^{\text{оиу}})\cdot\vartheta_{\zeta}^{\rho^{\text{исиб}}/\text{кнву}}(\tau^{\text{оиу}})\end{array}\right)}{\gamma_{\zeta}^{\rho^{\text{исиб}}/\text{ронву}}(\tau^{\text{оиу}})\cdot\delta_{\zeta_{\text{окии}}^{\text{киу}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}}-1)};\\
\zeta=\overline{1,3},\ \rho^{\text{исиб}}=\overline{1,\mu^{\text{писиб}}},
\end{cases}
\tag{2}
$$

$$\begin{cases} \dfrac{dY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}}{d\tau^{\text{оиу}}} = k_{\zeta}^{\text{сопка/снду}} \cdot \left(DY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}}) - PY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}}) \right); \\ DY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}}) = \alpha_{\zeta}^{\varphi^{\text{сс}}/\text{нск}}(\tau^{\text{оиу}}) \cdot Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}} - 1); \\ PY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}}) = o_{\zeta}^{\varphi^{\text{сс}}/\text{нсу}}(\tau^{\text{оиу}}) \cdot Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}} - 1); \\ \alpha_{\zeta}^{\varphi^{\text{сс}}/\text{нск}}(\tau^{\text{оиу}}) = 1 + \beta_{\zeta}^{\varphi^{\text{сс}}/\text{пос}}(\tau^{\text{оиу}}) \cdot \nu_{\zeta}^{\varphi^{\text{сс}}/\text{ппк}}(\tau^{\text{оиу}}) \cdot \dfrac{\psi_{\zeta_{\text{окии}}^{\text{двика}}}^{\varphi^{\text{сс}}}(\tau^{\text{оиу}})}{\psi_{\zeta_{\text{окии}}^{\text{ика}}}^{\varphi^{\text{сс}}}(\tau^{\text{оиу}} - 1)}; \\ o_{\zeta}^{\varphi^{\text{сс}}/\text{нсу}}(\tau^{\text{оиу}}) = k_{\zeta}^{\varphi^{\text{сс}}/\text{виу}}(\tau^{\text{оиу}}) \cdot \dfrac{\left(\begin{array}{l} \omega_{\zeta_{\text{окии}}^{\text{пон}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}}) \cdot h_{\zeta_{\text{окии}}^{\text{ика}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}}) + \omega_{\zeta}^{\rho^{\text{исиб}}/\text{пон}}(\tau^{\text{оиу}}) \cdot \\ \cdot h_{\zeta}^{\rho^{\text{исиб}}/\text{ика}}(\tau^{\text{оиу}}) + \omega_{\zeta}^{\varphi^{\text{сс}}/\text{пон}}(\tau^{\text{оиу}}) \cdot h_{\zeta}^{\varphi^{\text{сс}}/\text{ика}}(\tau^{\text{оиу}}) \end{array} \right)}{\gamma_{\zeta}^{\varphi^{\text{сс}}/\text{роика}}(\tau^{\text{оиу}}) \cdot \psi_{\zeta_{\text{окии}}^{\text{ика}}}^{\varphi^{\text{сс}}}(\tau^{\text{оиу}} - 1)}; \\ \zeta = \overline{1,3},\ \rho^{\text{исиб}} = \overline{1, \mu^{\text{писиб}}},\ \varphi^{\text{сс}} = \overline{1, \varepsilon^{\text{цпсхксиб}}}, \end{cases} \tag{3}$$

где $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}} - 1)$, $Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}} - 1)$ – соответственно значение $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$ и $Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$ в момент времени $(\tau^{\text{оиу}} - 1)$, предшествующий $\tau^{\text{оиу}}$;

$\delta_{\zeta_{\text{окии}}^{\text{двкиу}}}^{\rho^{\text{исиб}}}$, $\psi_{\zeta_{\text{окии}}^{\text{двика}}}^{\varphi^{\text{сс}}}$ – соответственно количество известных уязвимостей и КА на объекты КИИ, контролируемые $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ, дополнительно включенных в используемые БД за интервал времени $\left[\tau^{\text{оиу}} - 1, \tau^{\text{оиу}}\right]$ (ед. изм. – соответственно число известных уязвимостей/ $\tau^{\text{оиу}}$ и число известных КА/ $\tau^{\text{оиу}}$);

$\delta_{\zeta_{\text{окии}}^{\text{киу}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}} - 1)$, $\psi_{\zeta_{\text{окии}}^{\text{ика}}}^{\varphi^{\text{сс}}}(\tau^{\text{оиу}} - 1)$ – соответственно значение $\delta_{\zeta_{\text{окии}}^{\text{двкиу}}}^{\rho^{\text{исиб}}}$ и $\psi_{\zeta_{\text{окии}}^{\text{двика}}}^{\varphi^{\text{сс}}}$ в момент времени $(\tau^{\text{оиу}} - 1)$, предшествующий $\tau^{\text{оиу}}$.

В целях решения (2, 3) и сокращения количества используемых аналитических выражений и логических условий введем следующие условные обозначения: $\beta_{\zeta}^{g/\text{пос}}$ – показатель, соответствующий $\beta_{\zeta}^{\rho^{\text{исиб}}/\text{пос}}$, либо $\beta_{\zeta}^{\varphi^{\text{сс}}/\text{пос}}$; $\nu_{\zeta}^{g/\text{ппк}}$ – показатель, соответствующий $\nu_{\zeta}^{\rho^{\text{исиб}}/\text{ппк}}$, либо $\nu_{\zeta}^{\varphi^{\text{сс}}/\text{ппк}}$; $k_{\zeta}^{g/\text{виу}}$ – коэффициент, соответствующий $k_{\zeta}^{\rho^{\text{исиб}}/\text{виу}}$, либо $k_{\zeta}^{\varphi^{\text{сс}}/\text{виу}}$; $\omega_{\zeta}^{g/\text{пон}}$ – показатель, соответствующий $\omega_{\zeta_{\text{окии}}^{\text{пон}}}^{\rho^{\text{исиб}}}$, либо $\omega_{\zeta}^{\rho^{\text{исиб}}/\text{пон}}$, либо $\omega_{\zeta}^{\varphi^{\text{сс}}/\text{пон}}$; $\gamma_{\zeta}^{g/\text{ро}}$ – показатель, соответствующий $\gamma_{\zeta}^{\rho^{\text{исиб}}/\text{ронву}}$, либо $\gamma_{\zeta}^{\varphi^{\text{сс}}/\text{роика}}$; $\vartheta_{\zeta}^{g/\text{кнву}}$ – количество, соответствующее $\vartheta_{\zeta_{\text{окии}}^{\text{кнву}}}^{\rho^{\text{исиб}}}$, либо $\vartheta_{\zeta}^{\rho^{\text{исиб}}/\text{кнву}}$; $h_{\zeta}^{g/\text{ика}}$ – количество, соответствующее $h_{\zeta_{\text{окии}}^{\text{ика}}}^{\rho^{\text{исиб}}}$, либо $h_{\zeta}^{\rho^{\text{исиб}}/\text{ика}}$, либо $h_{\zeta}^{\varphi^{\text{сс}}/\text{ика}}$.

Затем определим значения $\beta_{\zeta}^{g/\text{пос}}$, $\nu_{\zeta}^{g/\text{ппк}}$, $k_{\zeta}^{g/\text{виу}}$, $\omega_{\zeta}^{g/\text{пон}}$, $\gamma_{\zeta}^{g/\text{ро}}$, $\vartheta_{\zeta}^{g/\text{кнву}}$, $h_{\zeta}^{g/\text{ика}}$ в виде:

$$\beta_{\zeta}^{g/\text{пос}}(\tau^{\text{оиу}}) = \begin{cases} 1, \ \exists \left[\begin{array}{l} \left(\mathcal{J}_{\zeta}^{g/\text{кос}}(\tau^{\text{оиу}}) > 0 \right) \wedge \\ \wedge \left(\mathcal{X}_{\zeta_{\text{окии}}}^{g/\text{всо}}(\tau^{\text{оиу}}) = \mathcal{X}_{\zeta_{\text{окии}}}^{g/\text{во}}(\tau^{\text{оиу}}) \right) \end{array} \right]; \\ 0, \text{ иначе}, \end{cases} \tag{4}$$

$$\zeta = \overline{1,3},\ g = \overline{1,D},$$

где $\mathcal{J}_{\zeta}^{g/\text{кос}}$ – количество фактов (случаев) обращений специалиста по ИБ в интервале времени $\left[\tau^{\text{оиу}} - 1, \tau^{\text{оиу}}\right]$ к $\rho^{\text{исиб}}$, либо $\varphi^{\text{сс}}$ в целях конфигурирования их ПФ в ζ-м их РжФ (ед. изм. – число фак-

тов обращений специалиста по ИБ);

$\mathcal{X}_{\zeta_{\text{окии}}}^{g/\text{всо}}$, $\mathcal{X}_{\zeta_{\text{окии}}}^{g/\text{во}}$ – соответственно количество выполненных специалистом по ИБ и выпущенных соответствующим разработчиком обновлений БД известных уязвимостей объектов КИИ, либо обновлений используемой БД известных КА на объекты КИИ, контролируемые $\rho^{\text{исиб}}$, либо $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – соответственно число выполненных и выпущенных обновлений);

D – общее количество ИСИБ (СС), включенных в состав ГетСОПКА, причем $\mu^{\text{писиб}}+\varepsilon^{\text{цпсхксиб}}=D$;

$$\nu_{\zeta}^{g/\text{ппк}}(\tau^{\text{оиу}})=$$

$$\begin{cases} 1, \text{ при } \tau^{\text{оиу}}\geq\tau^{\text{окпк}}; \\ 0, \text{ при } \left[\left(\tau^{\text{оиу}}=\tau^{\text{оквсо}}\right)\vee\left(\tau^{\text{оквсо}}=\tau^{\text{окпк}}\right)\right]; \\ 1-\dfrac{\tau^{\text{окпк}}-\tau^{\text{оиу}}}{\tau^{\text{окпк}}-\tau^{\text{оквсо}}}, \text{ при } \tau^{\text{оквсо}}<\tau^{\text{оиу}}<\tau^{\text{окпк}}, \end{cases} \quad (5)$$

$$\zeta=\overline{1,3},\ g=\overline{1,D},$$

где $\tau^{\text{оквсо}}$ – момент времени окончания выполнения специалистом по ИБ всего количества обновлений БД известных уязвимостей объектов КИИ, либо обновлений используемой БД известных КА на объекты КИИ, контролируемые $\rho^{\text{исиб}}$, либо $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – в заданных единицах времени);

$\tau^{\text{окпк}}$ – момент времени окончания выполнения процедуры конфигурирования ПФ $\rho^{\text{исиб}}$, либо $\varphi^{\text{сс}}$ в ζ-м их РжФ, который определим в виде (ед. изм. – в заданных единицах времени):

$$\tau^{\text{окпк}}=\tau^{\text{оквсо}}+\bar{t}_{\zeta_{\text{окии}}}^{g/\text{одв}}\cdot\mathcal{L}_{\zeta_{\text{окии}}}^{g/\text{дв}}(\tau^{\text{оиу}}),$$
$$\zeta=\overline{1,3},\ g=\overline{1,D}, \quad (6)$$

где $\bar{t}_{\zeta_{\text{окии}}}^{g/\text{одв}}$ – среднее время, затрачиваемое специалистом по ИБ на обработку отдельной (произвольной) известной уязвимости, либо известной КА на определенные объекты КИИ, принадлежащих $\delta_{\zeta_{\text{двкиу}}\zeta_{\text{окии}}}^{\rho^{\text{исиб}}}$, либо $\psi_{\zeta_{\text{двика}}\zeta_{\text{окии}}}^{\varphi^{\text{сс}}}$, а также на выделение одного соответствующего актуального атрибута ПД, принадлежащего $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$, либо на формирование одного соответствующего актуального правила обнаружения ИИБ, принадлежащего $Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$ (ед. изм. – в заданных единицах времени);

$\mathcal{L}_{\zeta_{\text{окии}}}^{g/\text{дв}}$ – число известных уязвимостей определенных объектов КИИ, либо известных КА на определенные объекты КИИ, образующих $\delta_{\zeta_{\text{двкиу}}\zeta_{\text{окии}}}^{\rho^{\text{исиб}}}$, либо $\psi_{\zeta_{\text{двика}}\zeta_{\text{окии}}}^{\varphi^{\text{сс}}}$;

$$k_{\zeta}^{g/\text{виу}}(\tau^{\text{оиу}})=\frac{\mathcal{I}_{\zeta}^{g/\text{ст}}(\tau^{\text{оиу}})}{\sum_{g=1}^{D}\mathcal{I}_{\zeta}^{g/\text{ст}}(\tau^{\text{оиу}})},$$
$$\zeta=\overline{1,3},\ g=\overline{1,D}, \quad (7)$$

где $\mathcal{I}_{\zeta}^{g/\text{ст}}$ – объем передаваемого $\rho^{\text{исиб}}$ в адрес $\varphi^{\text{сс}}$, либо принимаемого $\varphi^{\text{сс}}$ от $\rho^{\text{исиб}}$, $\rho^{\text{исиб}}=\overline{1,\ \mu^{\text{писиб}}}$ в ζ-м их РжФ за интервал времени $\left[\tau^{\text{оиу}}-1,\ \tau^{\text{оиу}}\right]$ сетевого трафика с результатами (информацией о состоянии определенных объектов КИИ) ПФ $\rho^{\text{исиб}}$ (ед. изм. – килобайт/мегабайт и т.п.);

$$\omega_{\zeta}^{g/\text{пон}}(\tau^{\text{оиу}})=\begin{cases}1,\ \mathcal{J}_{\zeta}^{g/\text{кон}}(\tau^{\text{оиу}})>0; \\ 0,\ \text{иначе},\end{cases} \quad (8)$$
$$\zeta=\overline{1,3},\ g=\overline{1,D},$$

где $\mathcal{J}_{\zeta}^{g/\text{кон}}$ – количество фактов (случаев) обращений внешнего и потенциального внутреннего непривилегированного нарушителей в интервале времени $\left[\tau^{\text{оиу}}-1,\ \tau^{\text{оиу}}\right]$ к определенным (контролируемым $\rho^{\text{исиб}}$) объектам КИИ, либо к $\rho^{\text{исиб}}$, либо к $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – число фактов обращений нарушителей);

$$\gamma_{\zeta}^{g/\text{ро}}(\tau^{\text{оиу}})=\left|\frac{\mathcal{B}_{\zeta}^{g/\text{всо}}(\tau^{\text{оиу}})}{\mathcal{B}_{\zeta}^{g/\text{во}}(\tau^{\text{оиу}})}\right|$$
$$\left[\begin{array}{l}\left(\mathcal{B}_{\zeta}^{g/\text{всо}}(\tau^{\text{оиу}})\geq 1\right)\wedge \\ \wedge\left(\mathcal{B}_{\zeta}^{g/\text{во}}(\tau^{\text{оиу}})\geq 1\right)\end{array}\right], \quad (9)$$
$$\zeta=\overline{1,3},\ g=\overline{1,D},$$

где $\mathcal{B}_{\zeta}^{g/\text{всо}}$, $\mathcal{B}_{\zeta}^{g/\text{во}}$ – соответственно количество выполненных специалистом по ИБ и выпущенных соответствующим разработчиком обновлений БД уязвимостей нулевого дня и впервые выявленных уязвимостей определенных (контролируемых $\rho^{\text{исиб}}$) объектов КИИ и $\rho^{\text{исиб}}$ ζ-м его РжФ, либо обновлений количества известных КА на определенные (контролируемые $\rho^{\text{исиб}}$) объекты КИИ, на $\rho^{\text{исиб}}$ (взаимодействующие с $\varphi^{\text{сс}}$) и на $\varphi^{\text{сс}}$ в ζ-м их РжФ, не включенных в используемую БД КА в связи с отсутствием сценариев их реализации (ед. изм. – соответственно число выполненных и выпущенных обновлений);

$\mathcal{B}_{\zeta}^{g/\text{всо}}(\tau^{\text{оиу}}) \geq 1$, $\mathcal{B}_{\zeta}^{g/\text{всо}}(\tau^{\text{оиу}}) \geq 1$ – соответственно область допустимых значений $\mathcal{B}_{\zeta}^{g/\text{всо}}$ и $\mathcal{B}_{\zeta}^{g/\text{всо}}$ в $\tau^{\text{оиу}}$ момент времени, указывающая на то, что при расчете значения $\gamma_{\zeta}^{g/\text{ро}}(\tau^{\text{оиу}})$ учитывается, что на этапе подготовке к эксплуатации ГетСОПКА специалистом по ИБ выполнена первоначальная актуализация соответствующего набора исходных данных, требуемых для реализации процедуры конфигурирования ПФ $\rho^{\text{исиб}}$, либо $\varphi^{\text{сс}}$, в результате чего исходные значения $\mathcal{B}_{\zeta}^{g/\text{всо}}$ и $\mathcal{B}_{\zeta}^{g/\text{во}}$ принимаются равными 1, которые впоследствии могут увеличиваются с течением времени;

$$\begin{cases} \vartheta_{\zeta}^{g/\text{кнву}}(\tau^{\text{оиу}}) \Big| \exists \tau^{\text{вкнву}}: \\ \quad \Big[\left(\tau^{\text{вкнву}} \leq \tau^{\text{нон}}\right) \vee \\ \vee \left(\tau^{\text{нон}} < \tau^{\text{вкнву}} \leq \tau^{\text{оон}}\right)\Big] \leq \tau^{\text{оиу}}; \\ h_{\zeta}^{g/\text{ика}}(\tau^{\text{оиу}}) \Big| \exists \tau^{\text{вика}}: \\ \quad \Big[\left(\tau^{\text{вика}} \leq \tau^{\text{нон}}\right) \vee \\ \vee \left(\tau^{\text{нон}} < \tau^{\text{вика}} \leq \tau^{\text{оон}}\right)\Big] \leq \tau^{\text{оиу}}; \\ \zeta = \overline{1,3},\ g = \overline{1,D}, \end{cases} \quad (10)$$

где $\tau^{\text{вкнву}}$, $\tau^{\text{вика}}$ – соответственно момент времени выявления (выпуска соответствующим разработчиком) уязвимостей нулевого дня и впервые выявленных уязвимостей определенных (контролируемых $\rho^{\text{исиб}}$) объектов КИИ, либо $\rho^{\text{исиб}}$ в ζ-м его РжФ, либо известных КА на определенные (контролируемые $\rho^{\text{исиб}}$) объекты КИИ, либо на $\rho^{\text{исиб}}$ (взаимодействующие с $\varphi^{\text{сс}}$) или на $\varphi^{\text{сс}}$ в ζ-м их РжФ, не включенных в используемую БД КА в связи с отсутствием сценариев их реализации (ед. изм. – в заданных единицах времени);

$\tau^{\text{нон}}$, $\tau^{\text{оон}}$ – соответственно момент времени начала и окончания обращения внешнего и потенциального внутреннего непривилегированного нарушителей к определенным (контролируемым $\rho^{\text{исиб}}$) объектам КИИ, либо к $\rho^{\text{исиб}}$, либо к $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – в заданных единицах времени).

На основе (2-10) определим текущий уровень информационной устойчивости ПФ ПИСИБ и ЦПСХКСИБ на этапе их эксплуатации в ζ-м РжФ при ДПВ и ДНПВ, направленных на нарушение их ПФ и доступности, посредством расчета текущих значений скоростей изменения набора (количества) данных (параметров) конфигурации (настройки) их ПФ (соответственно $dY_{\zeta}^{\text{писиб/пдк}} / dt$ и $dY_{\zeta}^{\text{цпсхксиб/пдк}} / dt$) в виде:

$$\begin{cases} \dfrac{dY_{\zeta}^{\text{писиб/пдк}}}{dt} = \min\limits_{\rho^{\text{исиб}}} \dfrac{dY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}}{d\tau^{\text{оиу}}}; \\ \dfrac{dY_{\zeta}^{\text{цпсхксиб/пдк}}}{dt} = \min\limits_{\varphi^{\text{сс}}} \dfrac{dY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}}{d\tau^{\text{оиу}}}; \end{cases} \quad (11)$$

$$\zeta = \overline{1,3},\ \rho^{\text{исиб}} = \overline{1,\mu^{\text{писиб}}},\ \varphi^{\text{сс}} = \overline{1,\varepsilon^{\text{цпсхксиб}}}.$$

В завершении учитывая (1, 11), определим текущее значение $dY_{\zeta}^{\text{сопка/пдк}} / dt$ в виде:

$$\frac{dY_{\zeta}^{\text{сопка/пдк}}}{dt} = \quad (12)$$

$$= \begin{cases} \dfrac{dY_{\zeta}^{\text{писиб/пдк}}}{dt} + \dfrac{dY_{\zeta}^{\text{цпсхксиб/пдк}}}{dt}, \text{ при } \left[\left(\left(\dfrac{dY_{\zeta}^{\text{писиб/пдк}}}{dt} \geq 0 \right) \wedge \left(\dfrac{dY_{\zeta}^{\text{цпсхксиб/пдк}}}{dt} \geq 0 \right) \right) \vee \left(\left(\dfrac{dY_{\zeta}^{\text{писиб/пдк}}}{dt} < 0 \right) \wedge \left(\dfrac{dY_{\zeta}^{\text{цпсхксиб/пдк}}}{dt} < 0 \right) \right) \right]; \\ \min\left(\dfrac{dY_{\zeta}^{\text{писиб/пдк}}}{dt}, \dfrac{dY_{\zeta}^{\text{цпсхксиб/пдк}}}{dt} \right), \text{ при } \left[\left(\dfrac{dY_{\zeta}^{\text{писиб/пдк}}}{dt} < 0 \right) \vee \left(\dfrac{dY_{\zeta}^{\text{цпсхксиб/пдк}}}{dt} < 0 \right) \right]; \\ \zeta = \overline{1,3}. \end{cases} \quad (12)$$

Анализируя представленный научно-методический аппарат оценивания информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в условиях ДПВ и ДНПВ, направленных на нарушение ее ПФ и доступности, в качестве направлений дальнейшего его развития следует определить необходимость в разработке:

- имитационной модели ПФ ГетСОПКА (например, на базе программной среды AnyLogic), способной обеспечить определение степени зависимости текущего уровня информационной устойчивости ПФ рассматриваемого объекта от текущих значений выделенных ключевых показателей с последующим формированием рекомендаций специалисту по ИБ по порядку администрирования ИСИБ (СС) в различных их РжФ, например, по направлению определения и соблюдения времени $t_{\zeta_{\text{окии}}}^{g/\text{одв}}$;
- формализованных подходов к определению уточненного семантического значения, показателей и критериев оценивания структурной и функциональной устойчивости ПФ рассматриваемого объекта в заданных РжФ и условиях эксплуатации, что совместно с его информационной устойчивостью позволит обоснованно сформировать комплексную (интегральную) количественную оценку в заданной предметной области с учетом определенных исходных данных по составу структурных элементов ГетСОПКА, а также устаревания ПД о текущем состоянии ПФ ИСИБ (СС) в выделенном временном интервале их адаптивного итерационного контроля;
- программной модели системы комплексного оценивания устойчивости ГетСОПКА на этапе ее эксплуатации в заданных РжФ и условиях эксплуатации, позволяющей оперативно формировать обоснованные ИТР на ФПУ ПФ рассматриваемого объекта.

Выводы

В работе предложен формализованный подход к оцениванию информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации при ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ее структурных элементов, в рамках которого:

1. На основе представления ГетСОПКА в виде кибернетической системы обосновано определено семантическое значение, показатель и критерий оценивания информационной устойчивости ПФ рассматриваемого объекта в заданных условиях эксплуатации, а также раскрыты и иные аспекты его устойчивости, в частности выделена структурная и функциональная устойчивость.

2. Приведено, что наиболее адекватным методом решения задачи оценивания информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в заданных условиях является метод системно-динамического моделирования, посредством которого построена системно-динамическая модель рассматриваемого объекта. При этом, сформирована система ключевых показателей, обеспечивающая возможность получения количественной оценки текущего уровня рассматриваемого аспекта устойчивости ГетСОПКА, а также сделан научно-технологический задел для оценивания ее структурной и функциональной устойчивости и, как следствие, формирования на их основе комплексной (интегральной) оценки.

3. На основе представление ГетСОПКА в виде системно-динамической модели посредством применения аналитических методов (дифференциальных уравнений, алгебраических выражений и логических условий) сформирована целенаправленная последовательность действий для получения количественной оценки текущего уровня информационной устойчивости ПФ рассматриваемого объекта в заданных РжФ и условий эксплуатации.

4. Определены планируемые направления развития разработанного научно-методического аппарата оценивания информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации, связанные с построением имитационной модели ПФ рассматриваемого объекта на базе программной среды AnyLogic, с формализацией подходов к комплексному оцениванию устойчивости ГетСОПКА с последующей разработкой соответствующей программной модели, обеспечивающей возможность практической реализации ПФПУ ПФ рассматриваемого объекта.

Литература

1. Котенко И.В., Саенко И.Б., Захарченко Р.И., Величко Д.В. Подсистема предупреждения компьютерных атак на объекты критической информационной инфраструктуры: анализ функционирования и реализации // Вопросы кибербезопасности. 2023. № 1(53). С. 13–27. DOI:10.21681/2311-3456-2023-1-13-27.
2. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. профессора РАН, доктора технических наук Д.П. Зегжды. – М.: Горячая линия – Телеком, 2022. 560 с.
3. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. – М.: Горячая линия – Телеком, 2023. 240 с.
4. Коноваленко С.А., Королев И.Д., Секунов В.Г. Моделирование системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Информационные системы и технологии. 2022. № 1(129). С. 105–113.
5. Устройство аудита информационной безопасности в автоматизированных системах: пат. 180789 Рос. Федерация / заявитель, патентообладатель Таразевич Е.С., Володина Н.И, Рыжов Б.С., Киселев В.В., Федеральное государственное бюджетное учреждение «4 Центральный научно-исследовательский институт» Министерства обороны Российской Федерации. – № 2017137955; заявл. 31.10.2017, опубл. 22.06.2018, Бюл. № 18. – 10 с.
6. Минаев В.А., Королев И.Д., Коноваленко С.А., Васильев Д.С., Секунов В.Г. Структурно-функциональная модель имитации компьютерных атак на автоматизированные системы // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ, управление. 2020. № 1. С. 3-16. DOI: 10.25586/RNU.V9187.20.01.P.003.
7. Коноваленко, С.А. Модель адаптивного контроля системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Информация и безопасность. 2022. Т. № 25. № 1. С. 141–154. DOI: 10.36622/VSTU.2022.25.1.012.
8. Коноваленко С.А. Функциональная модель синтеза скрипта контроля системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Вопросы защиты информации. 2022. № 2 (137). С. 3–12. DOI: 10.52190/2073-2600_2022_2_3.
9. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. 337 с.
10. Михайлов Р.Л., Макаренко С.И. Оценка устойчивости сети связи в условиях воздействия на нее дестабилизирующих факторов // Системы, сети и устройства телекоммуникаций. 2013. № 4. С. 69–79.
11. Мальцев В.А. Анализ устойчивости как комплексного функционального свойства системы технического обслуживания и ремонта военной техники // Известия ТулГУ. Технические науки. 2019. № 4. С. 215–221.
12. Цифровые двойники: монография / под ред. П.А. Созинова. – М.: Радиотехника, 2022. С. 113–232.
13. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Структурно-функциональная модель киберпространства // Вопросы кибербезопасности. 2021. № 4(44). С. 16–24. DOI:10.21681/2311-3456-2021-4-16-24.
14. Минаев В.А., Сычев М.П., Вайц Е.В., Киракосян А.Э. Имитационное моделирование эпидемий компьютерных вирусов // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2019. № 3. С. 3–12. DOI: 10.25586/RNU.V9187.19.03.P.003.

15. Минаев В.А., Сычев М.П., Вайц Е.В., Бондарь К.М. Системно-динамическое моделирование сетевых информационных операций // Инженерные технологии и системы. 2019. Т. № 29. № 1. С. 20–39. DOI: 10.15507/2658-4123.029.201901.020-039.
16. Коноваленко С.А. Модель системы комплексного оценивания устойчивости гетерогенной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на этапе ее эксплуатации / Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2023. № 3-4 (177-178). С. 71–81. DOI: 10.53816/23061456_2023_3–4_71.

METHODOLOGY FOR ASSESSING THE INFORMATION STABILITY OF A HETEROGENEOUS COMPUTER ATTACK DETECTION SYSTEM

Konovalenko S.A.[21]

The purpose of the study: *to determine the refined semantic meaning, indicator and criterion for assessing the information stability of the process of functioning of a heterogeneous system for detecting, preventing and eliminating the consequences of computer attacks, as well as the formation on their basis of a targeted sequence of actions to obtain a quantitative assessment of the aspect of stability under consideration.*

Research method: *system analysis, system dynamic modeling using algebraic expressions and logical conditions.*

Research results: *the need to develop a scientific and methodological apparatus for assessing the information stability of the process of functioning of a heterogeneous system for detecting, preventing and eliminating the consequences of computer attacks at the stage of its operation under conditions of destructive influences aimed at disrupting its process of functioning and availability has been determined. An analysis of the conceptual apparatus was carried out and terminological vagueness in the subject area under study was identified. A refined semantic meaning, indicator and criterion for assessing the information stability of the process of functioning of the object under consideration under given operating conditions has been generated. Based on the representation of a given object of assessment in the form of a cybernetic system and a system-dynamic model, a system of key indicators and a targeted sequence of actions have been developed to obtain a quantitative assessment of the current level of the sustainability aspect under consideration. Directions for the development of the developed scientific and methodological apparatus for assessing the information stability of the process of functioning of the object under consideration are proposed.*

The scientific novelty *lies in the provision of a theoretically justified formalized approach to assessing the information stability of the process of functioning of a heterogeneous system for detecting, preventing and eliminating the consequences of computer attacks, which, unlike the known ones, allows us to form a scientific and technological basis for obtaining a comprehensive assessment of the stability of a given object and the implementation of the proposed scientific and technical solutions on practice.*

Keywords: *cybernetic system, system-dynamic model, rate of change of information resource, vulnerability, computer attack, functional-parametric control procedures, disruption of the functioning process, disruption of accessibility.*

References

1. Kotenko I.V., Saenko I.B., Zakharchenko R.I., Velichko D.V. Subsystem for preventing computer attacks on critical information infrastructure objects: analysis of functioning and implementation // Issues of cybersecurity. 2023. No. 1(53). pp. 13-27. DOI:10.21681/2311-3456-2023-1-13-27.
2. Cybersecurity of the digital industry. Theory and practice of functional resistance to cyber attacks / Ed. Professor of the Russian Academy of Sciences, Doctor of Technical Sciences D.P. Zegrzdy. – M.: Hotline – Telecom, 2022. 560 p.

21 Sergey A. Konovalenko, Ph.D. (Technology), Krasnodar Higher Military Order of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: konovalenko_rcf@mail.ru

3. Erokhin S.D., Petukhov A.N., Pilyugin P.L. Security management of critical information infrastructures. – M.: Hotline – Telecom, 2023. 240 p.
4. Konovalenko S.A., Korolev I.D., Sekunov V.G. Modeling a system for detecting, preventing and eliminating the consequences of computer attacks // Information systems and technologies. 2022. No. 1(129). pp. 105-113.
5. Information security audit device in automated systems: Pat. 180789 Ross. Federation / applicant, patent holder E.S. Tarazevich, N.I. Volodina, B.S. Ryzhov, V.V. Kiselev, Federal State Budgetary Institution "4th Central Research Institute" of the Ministry of Defense of the Russian Federation. – No. 2017137955; appl. 31.10.2017, publ. 22.06.2018, Bulletin. No. 18. – 10 p.
6. Minaev V.A., Korolev I.D., Konovalenko S.A., Vasiliev D.S., Sekunov V.G. Structural-functional model for simulating computer attacks on automated systems // Bulletin of the Russian New University. Series: Complex systems: models, analysis, control. 2020. No. 1. pp. 3-16. DOI: 10.25586/RNU.V9187.20.01.P.003.
7. Konovalenko, S.A. Model of adaptive control of a system for detecting, preventing and eliminating the consequences of computer attacks // Information and Security. 2022. Vol. No. 25. No. 1. pp. 141-154. DOI: 10.36622/VSTU.2022.25.1.012.
8. Konovalenko S.A. Functional model for the synthesis of a control script for a system for detecting, preventing and eliminating the consequences of computer attacks // Issues of information protection. 2022. No. 2 (137). pp. 3-12. DOI: 10.52190/2073-2600_2022_2_3.
9. Makarenko S.I. Models of a communication system under conditions of deliberate destabilizing influences and reconnaissance. Monograph. – St. Petersburg: High-tech technologies, 2020. 337 p.
10. Mikhailov R.L., Makarenko S.I. Assessing the stability of a communication network under the influence of destabilizing factors // Systems, networks and telecommunication devices. 2013. No. 4. pp. 69-79.
11. Maltsev V.A. Analysis of stability as a complex functional property of the system of maintenance and repair of military equipment // Izvestia of Tula State University. Technical science. 2019. No. 4. pp. 215-221.
12. Digital twins: monograph / ed. P.A. Sozinov. – M.: Radio engineering, 2022. pp. 113-232.
13. Starodubtsev Yu.I., Zakalkin P.V., Ivanov S.A. Structural-functional model of cyberspace // Issues of cybersecurity. 2021. No. 4(44). pp. 16-24. DOI:10.21681/2311-3456-2021-4-16-24.
14. Minaev V.A., Sychev M.P., Vaits E.V., Kirakosyan A.E. Simulation modeling of computer virus epidemics // Bulletin of the Russian New University. Series: Complex systems: models, analysis and control. 2019. No. 3. pp. 3-12. DOI: 10.25586/RNU.V9187.19.03.P.003.
15. Minaev V.A., Sychev M.P., Vaitz E.V., Bondar K.M. System-dynamic modeling of network information operations // Engineering technologies and systems. 2019. Vol. No. 29. No. 1. pp. 20-39. DOI: 10.15507/2658-4123.029.201901.020-039.
16. Konovalenko S.A. Model of a system for comprehensive assessment of the stability of a heterogeneous system for detecting, preventing and eliminating the consequences of computer attacks at the stage of its operation / Questions of defense technology. Episode 16: Technical means of countering terrorism. 2023. No. 3-4 (177-178). pp. 71-81. DOI: 10.53816/23061456_2023_3–4_71.