УДК:004.056.53
Оригинальная статья
Надежность, том 20, №4, 2020 https://doi.org/10.21683/1729-2646-2020-20-4-35-41

Методика инструментально-расчетной оценки устойчивости объектов критической информационной инфраструктуры при информационно-технических воздействиях

Сергей Г. Антонов[1], **Иван И. Анциферов**[1], **Сергей М. Климов**[1]*
[1]4 ЦНИИ Минобороны России, Российская Федерация, Королев
*klimov.serg2012@yandex.ru

Сергей Г. Антонов

Иван И. Анциферов

Сергей М. Климов

Резюме. *Целью статьи является разработка методики, позволяющей получить количественную оценку показателей устойчивости объектов критической информационной инфраструктуры (КИИ) при информационно-технических воздействиях (ИТВ) с использованием данных по результатам экспериментальных исследований на стендовом полигоне. К объектам КИИ относятся информационно-телекоммуникационные сети (ИТКС), информационные системы (ИС), автоматизированные системы (АС) и системы электросвязи, которые применяются в компьютеризированных системах транспорта, энергетики, связи, навигации, промышленном производстве и других областях жизнедеятельности. Под устойчивостью функционирования объектов КИИ в статье понимается способность элементов объектов КИИ сохранять значения параметров функционирования в пределах установленных требований на заданном интервале времени при реализации ИТВ нарушителем. В качестве угроз ИТВ нарушителя – компьютерных атак – рассматриваются целенаправленные программно-аппаратные воздействия, приводящие к нарушению (блокированию, искажению) информационно-вычислительных процессов функционирования объектов КИИ на заданном интервале времени. Разработанная методика основана на экспериментальных исследованиях, методах ускоренных испытаний и расчетных методах оценки устойчивости функционирования объектов КИИ, использованных применительно к специфике системного анализа процессов функционирования ИТКС, ИС и АСУ при имитации ИТВ нарушителя. В качестве показателей в методике предложены два основных типа показателей, вероятности возникновения сбоев и дополнительных (искусственных) сбоев при передаче данных между элементами объектов КИИ, вызванных ИТВ, и вероятности сбоев и дополнительных сбоев в результате ИТВ при обработке информации на объектах КИИ. Включение в состав методики показателей для оценки дополнительных сбоев, обусловленных ИТВ, дает возможность априорного анализа редких и внезапных событий нарушения устойчивости функционирования объектов КИИ. По результатам оценки обосновываются организационно-технические меры информационной безопасности для нейтрализации ИТВ на объекты КИИ. Использование методики предполагает наличие стендовых полигонов (опытных районов) для оценки устойчивости и реальной защищенности объектов КИИ, на которых размещены функциональные аналоги объектов КИИ, имитаторы ИТВ, комплексы средств защиты информации (СЗИ) и ликвидации последствий компьютерных инцидентов. Разработанная методика позволяет оценить значения показателей устойчивости – вероятности успешной передачи данных между элементами объекта КИИ и вероятности успешной обработки информации в элементе объекта КИИ в условиях сбоев на основе инструментально-расчетной оценки процессов функционирования элементов системы при имитации ИТВ на стендовом полигоне.*

Ключевые слова: *информационно-технические воздействия, объекты критической информационной инфраструктуры, сбои, устойчивость.*

Формат цитирования: *Антонов С.Г., Анциферов И.И., Климов С.М. Методика инструментально-расчетной оценки устойчивости объектов критической информационной инфраструктуры при информационно-технических воздействиях// Надежность. 2020. № 4. С. 35-41. https://doi.org/10.21683/1729-2646-2020-20-4-35-41*

Поступила *05.08.2020 г.* / **После доработки** *21.08.2020 г.* / **К печати** *18.12.2020 г.*

Введение

Развитие объектов критической информационной инфраструктуры (КИИ) характеризуется интенсивным внедрением новых информационных технологий распределенного сбора, обработки, хранения и передачи значительных объемов разнородных данных в интересах эффективного управления промышленными и производственными процессами в различных сферах деятельности человека и государства [13, 14].

Значительный объем сетевых протоколов и данных на объектах КИИ, стандартные настройки параметров средств защиты информации (СЗИ) объективно приводят к внесению в них множества уязвимостей. Множество потенциальных уязвимостей в элементах объектов КИИ включает параметры уязвимостей программного обеспечения, информационного обеспечения, телекоммуникационного оборудования, а также параметры функциональных и сетевых уязвимостей.

Совокупность уязвимостей в элементах объектов КИИ создает предпосылки для реализации потенциальных внутренних и внешних угроз информационно-технических воздействий (ИТВ) нарушителя, которые снижают устойчивость функционирования объектов КИИ [1, 2, 6, 12].

В статье рассматриваются угрозы ИТВ нарушителя, представляющие собой целенаправленные программно-аппаратные воздействия, приводящие к нарушению устойчивости функционирования объектов КИИ. Реализация ИТВ нарушителем осуществляется в форме взаимосвязанных и многошаговых воздействий средствами фаззинга, компьютерных атак «отказ в обслуживании» (DDoS-атак) и информационной нагрузки [7].

Последствия успешной реализации ИТВ нарушителя на объекты КИИ характеризуются следующим:

- несанкционированный доступ к защищаемой информации на объектах КИИ;
- нарушение устойчивости функционирования;
- сбои и отказы в процессах выполнения информационно-расчетных задач;
- замедления при передаче технологической информации о состоянии элементов объектов КИИ;
- блокирование (нарушение) сетевого взаимодействия элементов объектов КИИ;
- возможность искажения информации, критической для применения объектов КИИ;
- инициализация недекларированных возможностей для запуска массированных ИТВ на элементы объектов КИИ РВСН, сопоставимых по последствиям с техногенными катастрофами.

В соответствии с современными требованиями в области информационной безопасности при обеспечении безопасности информации объектов КИИ необходимо обеспечить устойчивость функционирования при осуществлении в отношении их ИТВ нарушителя [10, 11, 13, 14].

Для повышения устойчивости функционирования объектов КИИ при ИТВ нарушителя необходима заблаговременная и экспериментальная оценка их реальной защищенности и устойчивости на стендах или опытных участках [3, 4, 9].

Проведение стендовых испытаний и оценки реальной защищенности и устойчивости объектов КИИ при ИТВ обеспечат подготовку, выбор обоснованных организационно-технических мер информационной безопасности по устранению уязвимостей и снижению вероятности реализации угроз ИТВ, что позволит повысить устойчивость функционирования элементов объектов КИИ за счет выполнения указанных мер.

Таким образом, разработка методики, позволяющей повысить устойчивость функционирования объектов КИИ при ИТВ нарушителя за счет априорной оценки и многовариантного выбора организационно-технических мер информационной безопасности, устранения уязвимостей, является актуальной и представляет практический интерес.

Постановка задачи

Для обоснования инструментально-расчетной оценки устойчивости объектов КИИ при ИТВ в условиях сбоев сделаны следующие предположения:

- усложнение структуры, состава, количества решаемых целевых задач, сохранение одновременно работоспособных подсистем различных поколений, организация информационного взаимодействия между удаленными элементами объектов КИИ при ИТВ нарушителя создают предпосылки для возможных сбоев и требуют оценки для поддержания необходимого уровня устойчивости объектов КИИ;
- случайный характер вскрытия уязвимостей нарушителем и проникновения ИТВ на объекты КИИ приводят к необходимости многовариантного имитационного моделирования угроз ИТВ нарушителя;
- выполнение только аналитическими расчетами оценки устойчивости объектов КИИ в условиях сбоев, вызванных ИТВ нарушителя, затруднительно, требуется натурное моделирование значимых элементов КИИ в регламентах работы, близких к реальным процессам функционирования;
- инструментальная оценка устойчивости объектов КИИ при имитации ИТВ носит характер контрольной проверки, по результатам которой устанавливается, что значения вероятностных показателей устойчивости в условиях сбоев не ниже заданных;
- в ходе инструментальной проверки на стендовом полигоне проводятся ускоренные испытания элементов объектов КИИ, когда имитируются режимы информационной нагрузки, ускоряющие процесс возникновения сбоев;
- с учетом принимаемых мер по информационной безопасности объектов КИИ, значения показателей вероятности устойчивого функционирования в условиях низко интенсивных сбоев могут быть настолько малы,

что потребуют значительного времени тестирования системы, что обусловливает важность расчетного прогноза по результатам инструментальной оценки [8, 11, 13];

- продолжительность инструментальной оценки осуществляется в течение времени, которое необходимо для достоверной оценки вероятностных показателей устойчивости объектов КИИ при допустимых значениях их средней наработки на сбой [14];

- использование имитатора ИТВ позволяет проводить ускоренные испытания объектов КИИ в ходе инструментально-расчетной оценки, так как на стенде имитируются факторы повышения интенсивности искусственных сбоев (повышение вероятности их возникновения) при форсированных режимах эксплуатации объектов КИИ.

В общем виде постановка научной задачи оценки устойчивости объектов КИИ при ИТВ нарушителя представлена следующим образом:

Дано:

$w_р$ – число реальных сбоев при передаче данных между элементами объекта КИИ;

$h_р$ – число реальных сбоев в средствах обработки информации на объектах КИИ;

$\Delta t_{СПД}$ – среднее время передачи данных между элементами объекта КИИ;

$\Delta t_{ПАК}$ – среднее время обработки информации в средствах объекта КИИ.

Требуется:

найти такие значение фактических параметров сбоев в объектах КИИ: числа $w_д^*$ дополнительных сбоев в сети передачи данных (СПД), числа $h_д^*$ дополнительных сбоев в системе обработки данных (СОД), времени $t_{СПД}^{СБ*}$ сбоя в СПД и времени $t_{ПАК}^{СБ*}$ сбоя в СОД, при которых сохраняются требуемые значения вероятности устойчивости функционирования

$$P_{УПАК}^{*} \geq P_{УПАК}^{ТРЕБ}\left[\left(w_р^{*}, w_д^{*}, t_{СПД}^{СБ*}\right), \left(h_р^{*}, h_д^{*}, t_{ПАК}^{СБ*}\right), \left(\Delta t_{СПД}^{*}, \Delta t_{ПАК}^{*}\right)\right]$$

при ограничениях на характеристики средств передачи и обработки данных в объектах КИИ:

$$\Delta t_{СПД} \in T_{СПД}, \Delta t_{ПАК} \in T_{ПАК}.$$

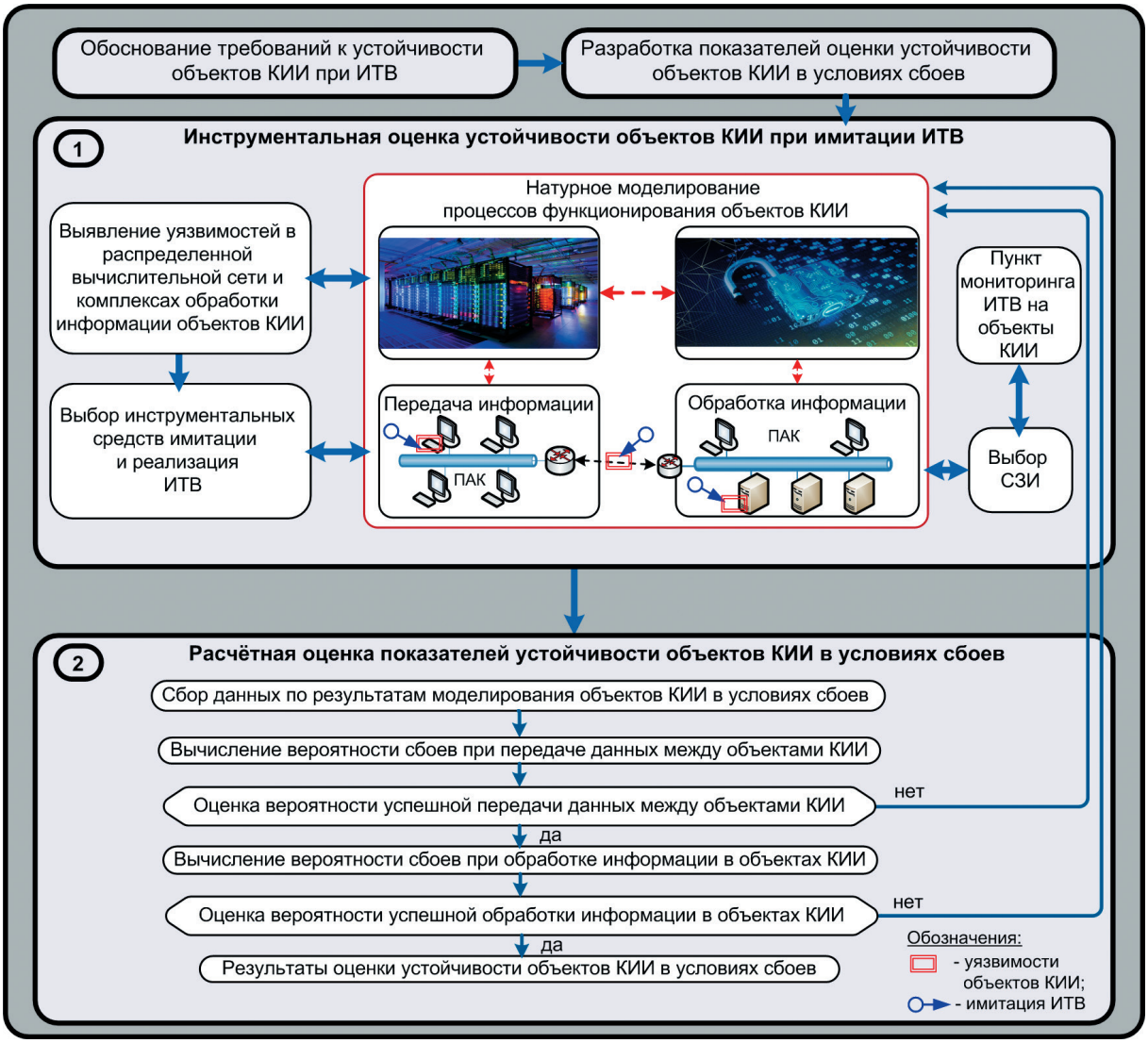

Рис. 1. Схема методики инструментально-расчетной оценки устойчивости объектов КИИ при имитации ИТВ

Постановка научной задачи исследований выполнена в предположении того, что процессы функционирования объектов КИИ представляются Марковскими процессами, а процессы ИТВ, приводящие к дополнительным сбоям, описываются распределением Пуассона.

Схема методики инструментально-расчетной оценки устойчивости объектов КИИ при ИТВ представлена на рис. 1. Под сбоем в элементах объектов КИИ будем понимать кратковременное (от нескольких секунд до 60 минут, с учетом времени восстановления) нарушение параметров функционирования [1, 8, 14]. В связи с тем, что категорированные объекты КИИ являются опасными для жизнедеятельности и их нарушение приводит к значительному ущербу, в исследованиях принято, что в объектах КИИ отказ недопустим. То есть, при ИТВ события нарушения работоспособности объектов КИИ на время более 60 минут нейтрализуются выбранными организационно-техническими мерами информационной безопасности, средствами восстановления работоспособности и резервными элементами.

По своей сути представленная методика обеспечивает подтверждение соответствия показателей устойчивости перспективных или модернизированных объектов КИИ в условиях сбоев, обусловленных ИТВ нарушителя, предъявленным техническим требованиям заказчика.

Для формирования доказательной базы соответствия реальных показателей устойчивости объектов КИИ в условиях сбоев полученным оценкам, в методике использована проверка соответствия результатов натурного и имитационного моделирования на стендовом полигоне расчетным оценкам выбранных показателей.

В методике предложена пошаговая последовательность определения показателей в ходе инструментально-расчетной оценки устойчивости функционирования объектов КИИ в условиях сбоев, включающей два основных этапа:

I. Инструментальная оценка устойчивости объектов КИИ при имитации ИТВ;

II. Расчетная оценка показателей устойчивости объектов КИИ в условиях сбоев.

Первоначально должно быть проведено обоснование требований к устойчивости функционирования объектов КИИ при ИТВ. Эти требования должны быть включены в тактико-техническое задание на опытно-конструкторскую работу по созданию объекта КИИ (экспериментального образца, опытного района объекта КИИ) или учтены при модернизации элементов объекта КИИ.

Далее в соответствии с методикой осуществляется разработка показателей для инструментально-расчетной оценки устойчивости объекта КИИ в условиях сбоев.

В связи с тем, что функционирование объекта КИИ характеризуется двумя основными процессами: передача данных между элементами объекта КИИ и обработка информации, то в методике предложены два показателя:

1. Вероятность успешной передачи данных между элементами объекта КИИ;

2. Вероятность успешной обработки информации в объекте КИИ.

Этап инструментальной оценки устойчивости функционирования объекта КИИ при имитации ИТВ проводится на стендовом полигоне и заключается в следующем:

1. Натурное моделирование процессов функционирования элементов объекта КИИ на стендовом полигоне или на опытном районе, включая передачу данных между элементами, а также обработку данных в локально-вычислительных сетях с программно-аппаратными комплексами (ПАК) на объектах КИИ.

2. Выбор средств защиты информации в соответствии с предъявленными требованиями к классам защищенности автоматизированных систем (АС), средств вычислительной техники, средств защиты информации от несанкционированного доступа, средств обнаружения вторжений, средств антивирусной защиты, межсетевых экранов, средств криптографической защиты, а также согласно требованиям к уровню доверия программного обеспечения АС [5].

3. Выявление уязвимостей в распределенной вычислительной сети и ПАК обработки информации объектов КИИ с использованием модели [8].

4. Выбор инструментальных средств имитации и реализация ИТВ с использованием методики [9].

Выходные статистические данные этапа инструментальной оценки устойчивости объектов КИИ при имитации ИТВ являются входными параметрами для расчетной оценки их устойчивости в условиях сбоев.

На этапе расчетной оценки устойчивости процессов функционирования объектов КИИ при имитации ИТВ с использованием метода ускоренных испытаний [14] сделаны предположения:

а) в составе объектов КИИ находятся два основных типа элементов:

1) *j*-е средства передачи данных объекта КИИ, в которых за время $t_{\text{СПД}j}$ с вероятностью $P_{\text{СПД}}^{\text{СБР}}$ происходят реальные сбои $w_{\text{р}j}$, а с вероятностью $P_{\text{СПД}}^{\text{СБД}}$ происходят дополнительные (искусственно созданные) сбои $w_{\text{д}j}$ при ИТВ нарушителя;

2) *i*-е средства обработки данных объекта КИИ, в которых за время $t_{\text{ПАК}i}$ с вероятностью $P_{\text{ПАК}}^{\text{СБР}}$ происходят реальные сбои $h_{\text{р}i}$, а с вероятностью $P_{\text{ПАК}}^{\text{СБД}}$ происходят дополнительные (искусственно созданные) сбои $h_{\text{д}i}$ при ИТВ нарушителя;

б) при передаче и обработке данных в объекте КИИ на каждом средстве выполняется технологическая операция, в ходе которой может произойти сбой;

в) вероятность возникновения сбоев в элементах объекта КИИ при выполнении технологических операций, как правило, имеет геометрическое распределение, которое аппроксимируется экспоненциальным законом распределения [14];

г) поток событий сбоев в средствах передачи и обработке данных объекта КИИ интерпретируется как непрерывный пуассоновский поток.

Этап расчетной оценки устойчивости нарушителя в условиях сбоев, произошедших в результате реализации ИТВ, методом ускоренных испытаний состоит из следующих шагов:

Шаг 1. Сбор данных по результатам моделирования объекта КИИ при имитации ИТВ, необходимых и достаточных параметров для проведения расчетной оценки устойчивости объекта КИИ в условиях сбоев.

Шаг 2. Вычисление вероятности сбоев при передаче данных между элементами объекта КИИ:

а) вычисление вероятности того, что произойдет $w_{рj}$ реальных сбоев при передаче данных между элементами объекта КИИ за время $t_{СПДj}$ в j-м средстве передаче данных:

$$P_{СПД}^{СБР}\left(w_{рj}\right)=\prod_{j=1}^{k} e^{-t_{СПДj}^{СБ} P_{СПДj}^{СБ}/\Delta t_{СПД}}\left(P_{СПДj}^{СБ}\right)^{w_{рj}}, \quad (1)$$

где $w_{рj}$ – число реальных сбоев в j-м средстве передачи данных;

$t_{СПДj}^{СБ}$ – время, за которое происходит сбой в j-м средстве передачи данных;

$P_{СПДj}^{СБ}$ – вероятность возникновения реального сбоя в j-м средстве передачи данных;

$\Delta t_{СПД}$ – среднее время передачи данных между элементами объекта КИИ;

k – число средств передачи данных.

б) вычисление вероятности того, что произойдет $w_{дj}$ дополнительных (искусственно организованных) сбоев при передаче данных между элементами объекта КИИ за время $t_{СПДj}$ в j-м средстве передачи данных:

$$P_{СПД}^{СБД}\left(w_{дj}\right)=\prod_{j=1}^{k} e^{-t_{СПДj}^{СБ} P_{СПДj}^{СБД}/\Delta t_{СПД}}\left(P_{СПДj}^{СБД}\right)^{w_{дj}}, \quad (2)$$

где $w_{дj}$ – число дополнительных сбоев в j-м средстве передачи данных;

$P_{СПДj}^{СБД}$ – вероятность возникновения дополнительного сбоя в j-м средстве передачи данных.

Шаг 3. Оценка вероятности успешной передачи данных между элементами объекта КИИ:

$$P_{УСПД}=\frac{1}{N_w}\sum_{j=1}^{N_w} U_{P_{УСПД}}\left(w_{рj},w_{дj}\right)\frac{\prod_{j=1}^{k} e^{-t_{СПДj}^{СБ} P_{СПДj}^{СБ}/\Delta t_{СПД}}\left(P_{СПДj}^{СБ}\right)^{w_{рj}}}{\prod_{j=1}^{k} e^{-t_{СПДj}^{СБ} P_{СПДj}^{СБД}/\Delta t_{СПД}}\left(P_{СПДj}^{СБ}\right)^{w_{дj}}}, \quad (3)$$

где N_w – количество инструментальных оценок на стендовом полигоне с реализацией векторов сбоев $w_{рj}$ и $w_{дj}$;

$U_{P_{УСПД}}\left(w_{рj},w_{дj}\right)$ – индикаторная функция, принимающая значение 1, если событие соответствует показателю $P_{УСПД}$, и 0 в противном случае.

Шаг 4. Вычисление вероятности сбоев при обработке информации в элементе объекта КИИ:

а) вычисление вероятности того, что произойдет $h_{рi}$ реальных сбоев при обработке информации на объекте КИИ за время $t_{ПАКi}$ в i-м ПАК:

$$P_{ПАК}^{СБР}\left(h_{рi}\right)=\prod_{i=1}^{l} e^{-t_{ПАКi}^{СБ} P_{ПАК}^{СБ}/\Delta t_{ПАК}}\left(P_{ПАКi}^{СБ}\right)^{h_{рi}}, \quad (4)$$

где $h_{рi}$ – число реальных сбоев в средствах обработки информации;

$t_{ПАКi}^{СБ}$ – время, за которое происходит сбой в i-м средстве обработки информации;

$P_{ПАКi}^{СБ}$ – вероятность возникновения реального сбоя в i-м средстве обработки информации;

$\Delta t_{ПАК}$ – среднее время обработки информации в средствах объекта КИИ;

l – число средств обработки информации.

б) вычисление вероятности того, что произойдет $h_{дi}$ дополнительных (искусственно организованных) сбоев при обработке информации на объекте КИИ за время $t_{ПАКi}$ в i-м ПАК:

$$P_{ПАК}^{СБД}\left(h_{дi}\right)=\prod_{i=1}^{l} e^{-t_{ПАКi}^{СБ} P_{ПАКi}^{СБД}/\Delta t_{ПАК}}\left(P_{ПАКi}^{СБД}\right)^{h_{дi}}, \quad (5)$$

где $h_{дi}$ – число дополнительных сбоев в средствах обработки информации;

$P_{ПАКi}^{СБД}$ – вероятность возникновения дополнительного сбоя в i-м средстве обработки информации.

Шаг 5. Оценка вероятности успешной обработки информации в элементе объекта КИИ:

$$P_{УПАК}=\frac{1}{N_h}\sum_{i=1}^{N_h} U_{P_{УПАК}}\left(h_{рi},h_{дi}\right)\frac{\prod_{i=1}^{l} e^{-t_{ПАКi}^{СБ} P_{ПАКi}^{СБ}/\Delta t_{ПАК}}\left(P_{ПАКi}^{СБ}\right)^{h_{рi}}}{\prod_{i=1}^{l} e^{-t_{ПАКi}^{СБ} P_{ПАКi}^{СБД}/\Delta t_{ПАК}}\left(P_{ПАКi}^{СБД}\right)^{h_{дi}}}, \quad (6)$$

где N_h – количество инструментальных оценок на стендовом полигоне с реализацией векторов сбоев $h_{рi}$ и $h_{дi}$;

$U_{P_{УПАК}}\left(h_{рi},h_{дi}\right)$ – индикаторная функция, принимающая значение 1, если событие соответствует показателю $P_{УПАК}$, и 0 в противном случае.

После выполнения шагов 1 – 5 методики формируются совокупность результатов оценки показателей устойчивости элементов объекта КИИ в условиях сбоев, которые будут использованы для повышения устойчивости объекта КИИ.

Табл. 1. Исходные данные для оценки вероятности успешной передачи данных между элементами типовых средств передачи данных объектов КИИ на базе протоколов TCP/IPв условиях ИТВ

Наименование характеристики процессов передачи данных между элементами типовых средств передачи данных объектов КИИ в условиях ИТВ	Значение характеристики
Среднее время передачи данных между элементами типовых средств передачи данных объектов КИИ	$\Delta t_{СПД}$ = 2, …, 16 сек
Число дополнительных сбоев в типовых средствах передачи данных объектов КИИ при ИТВ за 24 часа	$w_д$ = 1, …, 10
Среднее время, за которое происходит сбой в типовых средствах передачи данных объектов КИИ	$t_{СПД}^{СБ}$ = 2, 4, …, 24 часа

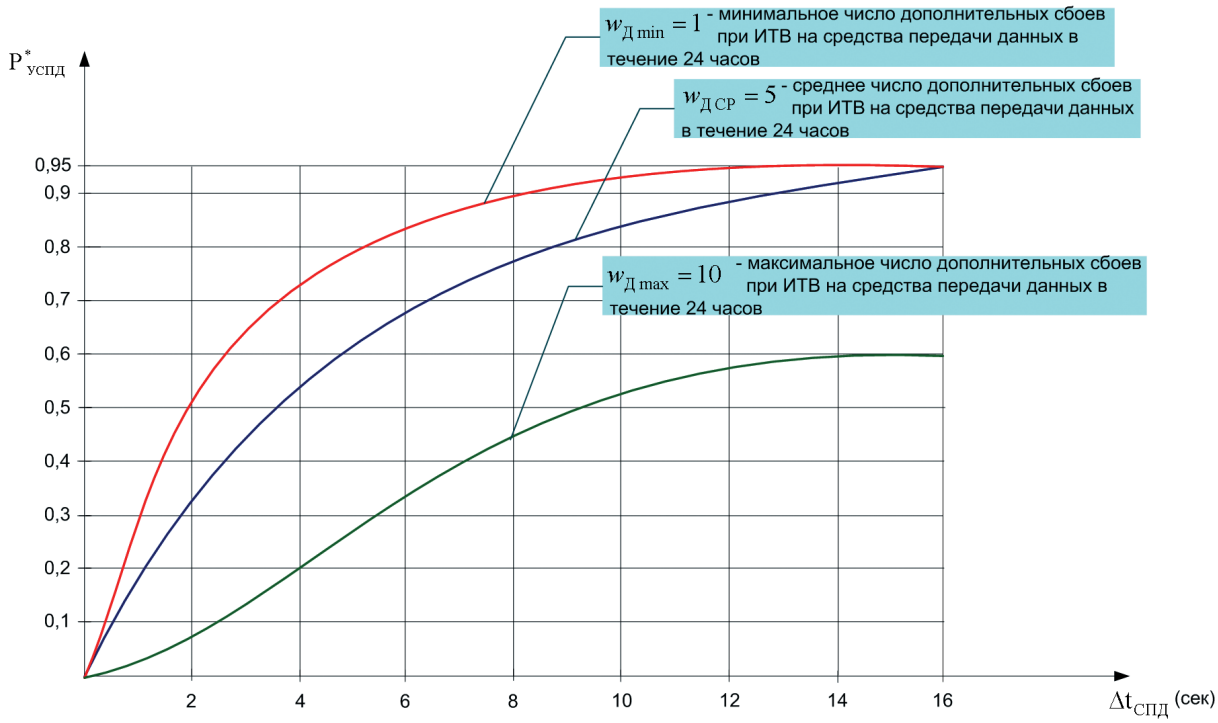

Рис. 2. Значения вероятности успешной передачи данных между элементами средств передачи данных объектов КИИ при изменении среднего времени передачи данных и числа дополнительных сбоев

В рамках исследований проведена предварительная оценка вероятности успешной передачи данных между элементами типовых средств передачи данных объектов КИИ на базе протоколов TCP/IP (исходные данные приведены в табл. 1). Результаты оценки влияния сбоев, вызванных ИТВ, на устойчивость элементов типовых средств передачи данных объектов КИИ представлены на рис. 2.

Анализ значений вероятностей успешной передачи данных между элементами типовых средств передачи данных объектов КИИ на базе протоколов TCP/IP в условиях ИТВ при изменении среднего времени передачи данных и числа дополнительных сбоев показывает следующее:

- вероятность успешной передачи данных между элементами типовых средств передачи данных объектов КИИ достигает значения 0,9 за 8 секунд при минимальном числе дополнительных сбоев при ИТВ нарушителя (1 сбой на суточном интервале работы);
- вероятность успешной передачи данных между элементами типовых средств передачи данных объектов КИИ принимает значение 0,8 за 10 секунд при среднем числе дополнительных сбоев при ИТВ нарушителя за счет применения средств резервирования и восстановления (5 сбоев на суточном интервале работы);
- вероятность успешной передачи данных между элементами типовых средств передачи данных объектов КИИ достигает лишь значения 0,6 за 16 секунд при максимальном числе дополнительных сбоев при ИТВ нарушителя даже при наличии средств ликвидации последствий компьютерных инцидентов (10 сбоев на суточном интервале работы).

В случае, когда ИТВ нарушителя своевременно обнаруживаются и нейтрализуются СЗИ на объекте КИИ, устойчивость функционирования средств передачи данных при дополнительных сбоях обеспечивается.

Вывод. Предложенная методика инструментально-расчетной оценки устойчивости объектов КИИ при ИТВ нарушителя позволяет оценить значения показателей устойчивости – вероятности успешной передачи данных между элементами объекта КИИ и вероятности успешной обработки информации в элементе объекта КИИ – в условиях сбоев на основе инструментально-расчетной оценки процессов функционирования элементов системы при имитации ИТВ на стендовом полигоне.

Библиографический список

1. Антонов С.Г., Климов С.М. Методика оценки рисков нарушения устойчивости функционирования программно-аппаратных комплексов в условиях информационно-технических воздействий // Надежность. 2017. Том 17. № 1. С. 32-39.

2. Антонов С.Г., Гордеев С.В., Климов С.М., Рыжов Б.С. Модели угроз совместных информационно-технических и информационно-психологических воздействий в гибридных войнах // Информационные войны. 2018. № 2 (46). С. 83-87.

3. Гапанович В.А., Шубинский И.Б., Замышляев А.М. Метод оценки рисков системы из разнотипных элементов // Надежность. 2016. Том 16. № 2. С.49-53.

4. Гапанович В.А., Розенберг Е.Н., Шубинский И.Б. Некоторые положения отказобезопасности и киберза-

щищенности систем управления // Надежность. 2014. № 2. С. 88-100.

5. ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. М.: Стандаинформ, 2016. 19 с.

6. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. М.: Стандаинформ, 2015. 7 с.

7. Климов С.М., Купин С.В., Купин Д.С. Модели вредоносных программ и отказоустойчивости информационно-телекоммуникационных сетей // Надежность. 2017. № 4. С. 36-43. DOI: 10.21683/1729-2640-2017-17-4

8. Климов С.М., Астрахов А.В., Сычев М.П. Методические основы противодействия компьютерным атакам: Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 2013. 110 с.

9. Климов С.М., Астрахов А.В., Сычев М.П. Технологические основы противодействия компьютерным атакам: Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 2013. 71 с.

10. Климов С.М., Половников А.Ю., Сергеев А.П. Модель функциональной отказоустойчивости процессов обеспечения потребителей навигационными сигналами в сложных условиях // Надежность. 2017. Том 17. № 2. С. 41-47.

11. Климов С.М., Поликарпов С.В., Федченко А.В. Методика повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий. // Надежность. 2017. Том 17. № 3. С. 32-40.

12. Климов С.М., Поликарпов С.В., Рыжов Б.С. и др. Методика обеспечения устойчивости функционирования критической информационной инфраструктур в условиях информационных воздействий // Вопросы кибербезопасности. 2019. № 6 (34). С. 37-48.

13. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза / И.Б. Шубинский. Ульяновск: Областная типография «Печатный двор», 2016. 544 с.

Сведения об авторах

Антонов Сергей Григорьевич – начальник отдела 4 ЦНИИ Минобороны России, Российская Федерация, Королев, e-mail: sergey_antonov_1960@mail.ru

Анциферов Иван Игоревич – научный сотрудник 4 ЦНИИ Минобороны России, Российская Федерация, Королев, e-mail: antsiferov-ivan@mail.ru

Климов Сергей Михайлович – доктор технических наук, профессор, начальник управления 4 ЦНИИ Минобороны России, Российская Федерация, Королев, e-mail: klimov.serg2012@yandex.ru

Вклад авторов в статью

Антонов С.Г. Разработка схемы и описания положений методики инструментально-расчетной оценки устойчивости объектов КИИ при имитации ИТВ. Проведение и анализ результатов экспериментальной оценки вероятности успешной передачи данных между элементами типовых средств передачи данных объектов КИИ.

Анциферов И.И. Формирование математической постановки задачи на разработку методики инструментально-расчетной оценки устойчивости объектов КИИ при ИТВ.

Климов С.М. Проведение системного анализа исходных допущений и разработка математических выражений для вычисления вероятностей сбоев при передаче данных между элементами объекта КИИ и успешной обработки информации в элементе объекта КИИ.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.