Методика оценки рисков нарушения устойчивости функционирования программно-аппаратных комплексов в условиях информационно-технических воздействий

Сергей Г. Антонов, 4 ЦНИИ Минобороны России, Королёв, Россия, e-mail: sergey_antonov_1960@mail.ru
Сергей М. Климов, 4 ЦНИИ Минобороны России, Королёв, Россия, e-mail: klimov.serg2012@yandex.ru

Сергей Г. Антонов

Сергей М. Климов

Резюме. Целью статьи является разработка методики, позволяющей получить количественную оценку уровня рисков нарушения устойчивости программно-аппаратных комплексов в условиях имитации информационно-технических воздействий и моделирования реального технологического цикла управления. В статье показана актуальность и важность методики оценки рисков устойчивости программно-аппаратных комплексов при реализации нарушителем целенаправленных и взаимосвязанных информационно-технических воздействий. В качестве информационно-технических воздействий рассматриваются целенаправленные и взаимосвязанные программно-аппаратные и программные воздействия с целью временного нарушения функционирования или логического вывода из строя программно-аппаратных комплексов. Условием успешной реализации информационно-технических воздействий является наличие в программно-аппаратных комплексах уязвимых мест, к которым относятся доступные для нарушителя IP, MAC-адреса и номера портов коммуникационного оборудования. Разработанная в статье методика базируется на следующем: оценка рисков осуществляется на стендовом испытательном полигоне или на реальных объектах с использованием соответственно стационарного и переносного комплексов имитации информационно-технических воздействий; риск нарушения устойчивости программно-аппаратных комплексов оценивается экспериментально как сочетание частоты и последствий, успешно реализованных информационно-технических воздействий; предварительная оценка рисков позволяет выбрать вариант средств защиты информации для устранения потенциальных уязвимостей; остаточный риск оценивается способностью программно-аппаратных комплексов ликвидировать последствия информационно-технических воздействий вариантами средств отказоустойчивости. В результате исследований предложена методика оценки рисков нарушения защищенности программно-аппаратных комплексов в условиях информационно-технических воздействий в виде логической последовательности шагов: анализа угроз информационно-технических воздействий; выявления уязвимостей; имитационного моделирования процессов функционирования комплексов в условиях информационно-технических воздействий на стендовом полигоне; выбора наилучших вариантов средств защиты информации от воздействий и отказоустойчивости комплекса; предварительной и окончательной оценки рисков нарушения устойчивости комплексов. В рамках методики разработаны вероятностно-временные показатели оценки рисков нарушения устойчивости программно-аппаратных комплексов обеспечивают возможность анализа ликвидации последствий угроз комплексных информационно-технических воздействий, выбора рациональных мер защиты информации и обеспечения отказоустойчивости. В составе методики предложена кубическая схема анализа устранения уязвимостей для критических элементов программно-аппаратных комплексов, которая позволяет определять необходимые для устранения уязвимости с учетом взаимосвязи интенсивности возникновения информационно-технических воздействий, уровней допустимого риска и уровнями эталонной модели взаимодействия открытых систем. Кроме того, разработан паспорт оценки степени рисков нарушения устойчивости программно-аппаратных комплексов по частоте успешно реализованных воздействий. В выводе отмечается, что разработанная методика позволяет на основе знаний о потенциальных уязвимостях и результатов экспериментальных исследований определить значение вероятностных показателей риска нарушения защищенности для установления наиболее опасных угроз и принятия соответствующих мер защиты информации.

Ключевые слова: программно-аппаратные комплексы, информационно-технические воздействия, риски нарушения устойчивости, средства защиты информации и обеспечения отказоустойчивости.

Формат цитирования: Антонов С.Г., Климов С.М. Методика оценки рисков нарушения устойчивости функционирования программно-аппаратных комплексов в условиях информационно-технических воздействий // Надежность. 2017. Т.17, №1. С. 32-39. DOI: 10.21683/1729-2646-2017-17-1-32-39

Введение

Рядом государств и хакерским сообществом активно создаются программные средства для подготовки, доставки и скрытного проникновения программного кода информационно-технических воздействий (ИТВ) (компьютерных атак) на автоматизированные системы управления технологическими процессами на транспорте, в энергетике, связи и других отраслях промышленности [4]. Базовыми элементами указанных автоматизированных систем являются программно-аппаратные комплексы (ПАК), взаимосвязанные между собой через коммуникационное оборудование и распределенные вычислительные сети.

В настоящее время ПАК представляют собой совокупность информационно-управляющих средств для организации сбора, обработки, выдачи управляющей информации в режиме реального времени и информационного взаимодействия органов управления с центрами обработки данных. В статье ПАК рассматриваются, прежде всего, как сложные и многофункциональные комплексы программ, а техническое оборудование – в качестве вычислительного ресурса необходимого для выполнения этих программ.

Распределенные вычислительные сети (РВС) на базе ПАК, по сути, представляют собой критически важные распределенные информационно-управляющие системы, которые являются потенциальными объектами для реализации ИТВ нарушителя.

Под ИТВ понимаются целенаправленные и взаимосвязанные программно-аппаратные и программные воздействия с целью временного нарушения функционирования или логического вывода из строя ПАК. Указанные воздействия можно считать разновидностью удаленных компьютерных атак вредоносного типа на информационное обеспечение, технологические процессы управления, компьютерное и коммуникационное оборудование сети ПАК [1].

Уязвимыми местами ПАК для ИТВ нарушителя являются доступные IP, MAC-адреса и номера портов коммуникационного оборудования. Потенциальные уязвимости рассматриваемых ПАК обусловлены:

а) использованием общедоступных протоколов передачи данных типа TCP/IP; телекоммуникационного оборудования магистральных каналов связи зарубежного производства с потенциальными недеklarированными возможностями и удаленным программным управлением; недоверенных программно-аппаратных платформ (импортных серверов, программных средств электронной почты, самообновляющихся операционных систем или их ядра);

б) возможными несанкционированными действиями внутреннего нарушителя по осуществлению преднамеренных и непреднамеренных ИТВ;

в) несогласованной и некачественной работой разнотипных элементов средств защиты информации (СЗИ).

В связи тем, что указанные уязвимости обуславливают потенциальную возможность для реализации ИТВ, приводящих к нарушению функционирования ПАК, разработка методики, позволяющей количественно оценить уровень рисков нарушения устойчивости ПАК в условиях имитации ИТВ, является актуальной.

Постановка задачи

В ходе исследований приняты следующие подходы:

- оценка рисков может осуществляться на стендовом испытательном полигоне или на реальных объектах с использованием соответственно стационарного и переносного комплексов имитации ИТВ;
- риск оценивается экспериментально по частоте успешно реализованных ИТВ;
- предварительная оценка риска позволяет выбрать вариант СЗИ от потенциальных уязвимостей;
- остаточный риск оценивается способностью ПАК ликвидировать последствия ИТВ вариантами средств отказоустойчивости (СОТ), то есть средствами восстановления работоспособности и резервирования функций и элементов ПАК.

На рисунке 1 представлена временная диаграмма процессов функционирования РВС на базе ПАК в условиях ИТВ в виде семи типовых периодов.

Особенность обеспечения устойчивого функционирования ПАК в условиях ИТВ состоит в том, что теоретически противодействие множеству ИТВ должно осуществляться СЗИ. В то же время, на практике СЗИ в лучшем случае лишь регистрируют факты реализации ИТВ на ПАК, а задачи обеспечения работоспособности и восстанавливаемости нарушенной системы не решаются. Следует отметить, что современные ИТВ, так называемые таргетированные компьютерные атаки, направлены, прежде всего, на вывод ПАК из строя – нарушение вероятностно-временных характеристик регламентов обработки информации. Последствия успешной реализации ИТВ на ПАК – кратковременные сбои (от нескольких секунд до 30 минут) и отказы (до нескольких часов) ПАК.

Оперативность (время) выполнения информационно-управляющих функций специального программного обеспечения (СПО) ПАК в условиях ИТВ является главным параметром его устойчивости функционирования.

На рисунке 1 приняты следующие обозначения:

t_{ϕ_m} – время функционирования РВС с ПАК; $t_{ИТВ_m}$ – время действия ИТВ нарушителя; $t_{по ИТВ_m}$ – время предупреждения и обнаружения ИТВ нарушителя; $t_{лп ИТВ_m}$ – время ликвидации последствий ИТВ.

Следовательно, суммарное время выполнения технологического цикла управления (ТЦУ) РВС с ПАК в условиях ИТВ можно определить выражением:

$$t_{ТЦУ} = \sum_{m=1}^N [t_{\phi_m} - (t_{ИТВ_m} + t_{по ИТВ_m} + t_{лп ИТВ_m})], \quad (1)$$

где $m = \{1, 2, \dots, N\}$ – натуральный ряд чисел.

Рисунок 1 – Временная диаграмма процессов функционирования РВС на базе ПАК в условиях ИТВ

При оценке рисков ПАК в условиях ИТВ необходимо осуществить следующее:

1. Выбор оцениваемых ПАК и определение степени детальности рассмотрения их характеристик на интервале ТЦУ.
2. Имитацию комплекса ИТВ на ПАК.
3. Обнаружение известных и неизвестных ИТВ в динамическом процессе функционирования ПАК.
4. Анализ ИТВ (параметрическая идентификация, каталогизация признаков и обновление базы данных ИТВ).
5. Выбор варианта средств защиты информации от ИТВ (противодействия ИТВ) и обеспечения отказоустойчивости ПАК (восстановления и резервирования).

С использованием современных методов противодействия ИТВ и управления рисками в критически важных информационных системах [1–3, 5–7] методику оценки рисков нарушения защищенности ПАК в условиях ИТВ представим следующей последовательностью шагов (рисунок 2):

1. Анализ комплексных угроз ИТВ.
2. Выявление уязвимостей в РВС с ПАК.

3. Имитационное моделирование процессов функционирования ПАК в условиях ИТВ на стендовом полигоне.

4. Выбор вариантов средств защиты информации от ИТВ.

5. Предварительная оценка рисков нарушения устойчивости ПАК с выбранными СЗИ (при реализации наилучшего варианта мер и средств защиты информации от ИТВ).

6. Выбор вариантов средств отказоустойчивости ПАК.

7. Контроль (окончательная оценка) остаточного риска с учетом выбранного варианта средств отказоустойчивости ПАК.

Комплексные угрозы ИТВ на ПАК включают в свой состав следующие имитируемые воздействия:

- компьютерные атаки типа «распределенный отказ в обслуживании» (DDoS – атаки);
- информационная нагрузка пакетами данных (множественными потоками со стандартными пакетами данных);
- фаззинг – воздействие нестандартными (с искаженными полями) пакетами данных;

Рисунок 2 – Схема методики оценки рисков нарушения защищенности ПАК в условиях ИТВ

- скрытно внедряемые и самораспространяющиеся вредоносные программы.

Шаг 1. Анализ комплексных угроз ИТВ предлагается построить на основе разработки классификации, подобной материалам [1], по классификационному признаку последствий воздействия ИТВ на ПАК. По указанному признаку определим ИТВ пяти типов:

- функциональное поражение (сбои и отказы) ПАК;
- разрыв соединений в информационно-управляющих каналах передачи данных;
- введение ложной информации (искажение информации);
- реализация информационной перегрузки ПАК;
- вскрытие доступных для ИТВ уязвимостей нулевого дня методом фаззинга (множественных потоков с семантически искаженными пакетами данных).

Шаг 2. Уязвимые места в РВС с ПАК для реализации имитационной модели угроз ИТВ определим с использованием ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» путем разработки типового паспорта уязвимостей ПАК (таблица 1).

В методике делается допущение о существовании потенциальных уязвимостей «нулевого дня» в про-

граммной реализации протоколов передачи данных, коммуникационном оборудовании, операционных системах, драйверах устройств и других компонентах РВС на базе ПАК на уровне 3-5% от возможных IP, MAC-адресов и номеров портов.

Шаг 3. Имитационное моделирование процессов функционирования ПАК в условиях ИТВ состоит в том, что на стендовом полигоне соответствующими средствами экспериментальным путем воспроизводятся взаимосвязанные процессы:

- штатного функционирования сегмента распределенной вычислительной сети с ПАК;
- имитации комплекса ИТВ нарушителя;
- противодействия ИТВ на основе различных вариантов применения СЗИ и СОТ.

Моделирование указанных процессов должно позволять проводить экспериментальные исследования и анализ сетевой защищенности ПАК в условиях ИТВ. Анализ сетевой защищенности ПАК осуществляется по семи уровням эталонной модели взаимодействия открытых систем (ЭМ ВОС) путем контроля реализации функций безопасности РВС на каждом из уровней. Для оценки рисков защищенности ПАК в условиях ИТВ наиболее важно проверить управление доступом к се-

тевым сервисам на транспортном, сеансовом и сетевом уровнях ЭМ ВОС.

Степень детализации имитационных моделей ПАК, ИТВ, СЗИ и СОТ должна обеспечивать возможность воспроизведения основных функций реальных объектов риска, проведения необходимого количества испытаний и получения статистических данных для оценки риска.

Шаг 4. К совокупности выбираемых СЗИ от ИТВ отнесем:

- средства обнаружения и предупреждения и компьютерных атак (СОПКА);
- межсетевые экраны (МЭ);
- ложные сетевые информационные объекты (ЛСИО);
- средства антивирусной защиты (САВЗ);
- автоматизированные модули доверенной загрузки (АМДЗ) – идентификация и аутентификация операторов.

Предположим, что в структуре РВС с ПАК циркулирует информация, относящаяся к информации ограниченного доступа. Тогда определим, что в предлагаемой методике рассматриваются СЗИ таких классов, которые обеспечивают защиту информации ограниченного доступа в РВС.

Шаг 5. Предварительная оценка рисков нарушения устойчивости ПАК с выбранными СЗИ.

В ходе выбора варианта мер и средств защиты информации от ИТВ должна быть осуществлена проверка уязвимости сетевой конфигурации и программного обе-

спечения сети, каждого из СЗИ на соответствие требованиям руководящих документов, а также произведена их общая оценка. Исходные данные для предварительной оценки рисков нарушения устойчивости ПАК с выбранными СЗИ и в условиях ИТВ следующие:

1. Вероятность обнаружения и идентификации комплексных ИТВ может принимать минимальные (0,2–0,4), среднее (0,5) и максимальные значения (0,7–0,9).

2. Вероятность реализации ИТВ на ПАК может принимать минимальные (0,2–0,4), среднее (0,5) и максимальные значения (0,7–0,9).

3. Варианты мер и средств защиты информации от ИТВ конечны (3-5 вариантов) и определяются возможными для применения в ПАК сертифицированными СЗИ (с учетом специфики его программно-аппаратной платформы).

Контроль требуемого уровня защиты информации ПАК в условиях ИТВ обеспечивается поддержанием значения вероятности выполнения ТЦУ за заданное время (для систем функционирующих в режимах близких к реальному масштабу времени) в условиях ИТВ не ниже требуемого (например, $R_{\text{треб}}=0,95$).

Комплексные ИТВ нарушают защищенность ПАК и, прежде всего, приводят к нарушению доступности и целостности информации, логики маршрутизации пакетов данных. Воздействия реализуются нарушителем только при наличии уязвимых мест в ПАК.

В ходе предварительной оценки рисков нарушения защищенности ПАК проверяется экспериментальным путем, насколько обеспечивается устойчивость функ-

Таблица 1 – Типовой паспорт уязвимостей ПАК

Элементы описания уязвимости ПАК	Описание уязвимости ПАК
1. Наименование уязвимости	Уязвимость ПАК «Оператор»
2. Идентификатор уязвимости	ПАК-2016-00007
3. Краткое описание уязвимости	Уязвимость допускает перехват управления ПАК
4. Класс уязвимости	Уязвимость операционной системы Windows
5. Наименование уязвимого элемента и его версия	Модули электронной почты в версии 10
6. Протокол передачи данных ПАК	Протокол обмена, прямой доступ к средствам управления ПАК
7. Особенности аппаратной и программной реализации ПАК	Аппаратно-программная платформа основана на технологиях клиент-сервер, гипервизора и программной виртуализации, протокол передачи данных TCP/IP версии v.6, специальное программное обеспечение версии 1.1
8. Тип недостатка	Недостатки, связанные с аутентификацией операторов
9. Место возникновения (проявления) уязвимости	Уязвимость существует из-за отсутствия проверки легитимности источника управления ПАК
10. Идентификатор типа недостатка	Нет данных
11. Дата выявления уязвимости	1.11.2016
12. Автор, опубликовавший информацию о выявленной уязвимости	Подразделение информационной безопасности
13. Способ (правило) обнаружения уязвимости	Выполнение пошаговой инструкции
14. Критерии опасности уязвимости	Превышение установленного значения вероятности риска
15. Степень опасности уязвимости	Высокая
16. Возможные меры по устранению уязвимости	Доработка средств защиты информации и протоколов информационного взаимодействия ПАК
17. Дополнительные сведения	В сети используется маршрутизатор Juniper

Таблица 2 – Паспорт оценки степени рисков нарушения устойчивости ПАК в условиях ИТВ

Частота возникновения ИТВ	Оценка степени риска ИТВ			Уровень риска возникновения ИТВ
	I вариант функции СОПКА минимальные	II вариант функции СОПКА на среднем уровне	III вариант функции СОПКА максимальные	
Маловероятное событие $P_{ИТВ} \leq 10^{-8}$ 1/ч	низкая баллы: 3	низкая баллы: 3	низкая баллы: 3	Малозначительный Сумма баллов: 9
Событие возможное $P_{ИТВ} \leq 10^{-7}$ 1/ч	низкая баллы: 3	средняя баллы: 5	высокая баллы: 7	Допустимый Сумма баллов: 15
Событие вполне вероятно $P_{ИТВ} \leq 10^{-6}$ 1/ч	средняя баллы: 5	высокая баллы: 7	высокая баллы: 7	Нежелательный Сумма баллов: 19
Вероятность события высокая $P_{ИТВ} \leq 10^{-5}$ 1/ч	средняя баллы: 5	высокая баллы: 7	очень высокая баллы: 10	Значительный Сумма баллов: 22
Вероятность события очень высокая $P_{ИТВ} \leq 10^{-4}$ 1/ч	высокая баллы: 7	высокая баллы: 7	очень высокая баллы: 10	Недопустимый Сумма баллов: 24
Событие произойдет наверняка $P_{ИТВ} \leq 10^{-3}$ 1/ч	высокая баллы: 7	очень высокая баллы: 10	очень высокая баллы: 10	Критический Сумма баллов: 27

ционирования элементов ПАК и СЗИ к сбоям и отказам в условиях ИТВ.

Предполагается, что процессы реализации ИТВ являются независимыми и распределены по экспоненциальному закону. Вероятность успешных ИТВ обуславливает риск возникновения сбоев и отказов ПАК.

Предварительная оценка рисков ПАК в условиях ИТВ включает:

- а) разработку показателей оценки рисков ПАК:
 - вероятность (частота) успешного осуществления ИТВ (в соответствии с табл. 2) – $P_{ИТВ}$;
 - вероятность успешного противодействия ИТВ – $P_{УП}$;
 - предполагаемый ущерб (уровни последствий от воздействий ИТВ табл. 2) – γ_i ;
 - значение риска нарушения защищенности ПАК от ИТВ равно произведению вероятности успешного осуществления ИТВ на предполагаемый ущерб – $R_{ИТВ_i}$;
- б) выбор доверительного интервала (границ допустимости) успешной реализации ИТВ на ПАК [5]:
 - определение доверительной вероятности:
 $P_{ИТВ}(\varepsilon) = \beta = 0,95$ – максимально достижимое значение для ПАК сложных систем [2], где ε – половина длины доверительного интервала;
 - определение интенсивности отказов ПАК в результате успешных ИТВ:

$$\lambda_{ИТВ_i} = \sum_{i=1}^m \frac{n_{Н\text{ ПАК}_i}}{N_{ПАК_i} t_{ИТВ_i}}, \quad (2)$$

где $\lambda_{ИТВ_i}$ – среднее число успешно реализованных ИТВ в единицу времени; $n_{Н\text{ ПАК}_i}$ – число нарушенных ПАК в РВС; $N_{ПАК_i}$ – общее количество ПАК в РВС; $t_{ИТВ_i}$ – длительность воздействия ИТВ; m – количество испытаний;

в) получение значения потенциального риска для варианта ПАК по соотношению (интенсивности возникновения сбоев и отказов в результате удачного исхода ИТВ):

$$R_{ИТВ_i}^{ПТР}(t_{ИТВ_i}) = \left[\prod_{i=1}^k (1 - e^{-\lambda_{ИТВ_i} t_{ИТВ_i}}) \right] \gamma_i, \quad (3)$$

где i – вариант ПАК; γ_i – величина ущерба от ИТВ (определяется с использованием суммы баллов в таблице 2).

При вычислении $R_{ИТВ_i}$ используется принцип – риск настолько низок, насколько это достижимо на практике.

Шаг 6. Выбор вариантов средств отказоустойчивости ПАК на основе применения средств резервирования (структурно-функциональной избыточности) и восстановления (временной избыточности на технологические циклы управления РВС с ПАК) с использованием материалов [1–3]:

а) обеспечение отказоустойчивости ПАК на основе применения средств восстановления (в предположении, что СОТ обеспечивает ликвидацию последствий ИТВ путем восстановления ПАК) определим выражением для вероятности восстановления:

$$P_{вос}^{СОТ}(t_{вос}) = \frac{\mu_{B_i}}{\lambda_{ИТВ_i} + \mu_{B_i}} + \frac{\lambda_{ИТВ_i}}{\lambda_{ИТВ_i} + \mu_{B_i}} e^{-(\lambda_{ИТВ_i} + \mu_{B_i}) t_{вос}}, \quad (4)$$

где, при условии экспоненциального закона распределения интенсивностей ИТВ и восстановления элементов ПАК, μ_{B_i} – интенсивность восстановления ПАК на основе i -го ИТВ;

б) обеспечение отказоустойчивости ПАК на основе применения средств резервирования определим выражением для коэффициента готовности:

$$K_{Г_i}^{ПАК} = \frac{1}{1 + m \frac{\lambda_{ИТВ_i}}{\mu_{B_i}}} P_{адап}, \quad (5)$$

где m – количество резервных элементов ПАК в РВС; $P_{адап} > 0,85-0,90$ – вероятность успешной адаптации ПАК к сбоям и отказам после реализации ИТВ.

Шаг 7. Контроль (окончательная оценка) остаточного риска с учетом выбранного варианта средств

отказоустойчивости ПАК заключается в том, что для выбранного варианта мер и СЗИ от ИТВ проводятся дополнительные оценки риска, позволяющие подтвердить, что указанные меры и СЗИ позволяют снизить риск до допустимого уровня (насколько это достижимо на практике).

Условием минимизации остаточного риска выбранного варианта отказоустойчивого ПАК в условиях ИТВ считается устранение уязвимостей, через которые могут быть реализованы воздействия, или нейтрализация ИТВ взаимосвязанным применением средств СЗИ и СОТ.

На рисунке 3 предложена кубическая схема анализа устранения уязвимостей для критических элементов ПАК, которая позволяет определять необходимые для устранения уязвимости с учетом взаимосвязи интенсивности возникновения ИТВ, допустимого уровня риска и уровнями ЭМ ВОС.

Порядок применения кубической схемы следующий:

а) выбирается один из семи уровней ЭМ ВОС (на схеме для примера выбран седьмой уровень), на котором рассматриваются критические элементы ПАК;

б) с использованием таблицы 1 определяются факты устранения или не устранения уязвимостей ПАК;

в) по правой части рисунка 3 (соответствия типов ИТВ доступным сетевым сервисам на уровнях ЭМ ВОС) выбираются возможные ИТВ для данного уровня;

г) на основе результатов экспериментов по таблице 2 определяется частота возникновения ИТВ;

д) определяется допустимый риск для критического элемента ПАК по математическому соотношению:

$$R_{ИТВ_j}^{ДР}(t_{ИТВ_j}) = \gamma_{ПАК_j} \prod_{j=1}^{K_3} [1 - P_{уяз_j}(t_{ИТВ_j}) P_{ИТВ_j}(t_{ИТВ_j})], \quad (6)$$

где $t_{ИТВ_j}$ – период времени реализации j -го ИТВ нарушителем; $\gamma_{ПАК_j}$ – ущерб от сбоя (отказа) критического элемента ПАК при j -м ИТВ; K_3 – количество экспериментов; $P_{уяз_j}(t_{ИТВ_j})$ – вероятность использования уязвимостей за время $t_{ИТВ_j}$, определяется экспертным путем или по статистическим данным эксплуатации РВС на базе ПАК; $P_{ИТВ_j}(t_{ИТВ_j})$ – вероятность успешной реализации j -го ИТВ за время $t_{ИТВ_j}$ нарушителя на критический элемент ПАК.

Наименьший возможный риск нарушения устойчивости ПАК в условиях ИТВ оценим с использованием критерия Сэвиджа:

$$R_{ПАК}(t_{ТЦУ}) = \max_i \min_j R_{ИТВ_j}(t_{ТЦУ}), \quad (7)$$

где i – вариант построения отказоустойчивого РВС с ПАК на основе применения СЗИ и СОТ; j – успешно осуществленное ИТВ на ПАК.

Заключение

В результате рассмотрения РВС на базе ПАК, являющихся потенциальными объектами для реализации ИТВ, в статье предложена методика, которая при решении задачи оценки реального уровня защищенности ПАК

Рисунок 3 – Кубическая схема анализа устранения уязвимостей для критических элементов ПАК

от ИТВ позволяет на основе знаний о потенциальных уязвимостях и результатов экспериментальных исследований определить значение вероятностных показателей риска нарушения защищенности для установления наиболее опасных угроз и принятия, соответствующих мер защиты информации.

Библиографический список

1. Климов С.М., Астрахов А.В., Сычев М.П. Технологические основы противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 71 с, 2013.
2. Климов С.М., Астрахов А.В., Сычев М.П. Методические основы противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 110 с, 2013.
3. Климов С.М., Астрахов А.В., Сычев М.П. Экспериментальная оценка противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 116 с, 2013.
4. Овчинский В.С. Новая стратегия кибербезопасности США. Международный научно-аналитический журнал «Стратегические приоритеты», выпуск 4 (8), 2015. – С. 15 – 32.
5. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа/ И.Б. Шубинский.

– Ульяновск: Областная типография «Печатный двор», 2012. – 216 с., ил.

6. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа/И.Б. Шубинский. – Ульяновск: Областная типография «Печатный двор», 2012. – 296 с., ил.

7. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза/ И.Б. Шубинский. – Ульяновск: Областная типография «Печатный двор», 2016. – 544 с., ил. – («Журнал надежность»).

Сведения об авторах

Сергей Г. Антонов – начальник отдела 4 ЦНИИ Минобороны России. 141092, Россия, Московская обл., г. Королёв, мкр. Юбилейный, ул. М.К.Тихонравова, д. 38/2, кв. 176, тел. + 7(916)788-57-92, e-mail: sergey_antonov_1960@mail.ru

Сергей М. Климов – доктор технических наук, профессор, начальник управления 4 ЦНИИ Минобороны России. 141092, Россия, Московская обл., г. Королёв, мкр. Юбилейный, ул. Б.Комитетская, д. 12, кв. 105, тел. +7 (985)928-13-55, e-mail: klimov.serg2012@yandex.ru.

Поступила 22.12.2016