ВОЕННО-ИНЖЕНЕРНАЯ КОРПОРАЦИЯ
РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
Секция «Инженерные проблемы стабильности и конверсии»

ISSN 1680-2780

Двойные технологии

№ 1
2020

III. ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

ДВОЙНЫЕ ТЕХНОЛОГИИ №1 (90) 2020

Научно-технический журнал
Наукоемкие технологии, проекты двойного использования комплексов вооружений, техногенная и другие виды безопасностей эксплуатации военных систем, экологический мониторинг.

Группы специальностей: авиационная и ракетно-космическая техника (05.07.00); радиотехника и связь (05.12.00); информатика, вычислительная техника и управление (05.13.00) (технические, физико-математические науки).

СОДЕРЖАНИЕ

РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
СЕКЦИЯ «ИНЖЕНЕРНЫЕ ПРОБЛЕМЫ СТАБИЛЬНОСТИ И КОНВЕРСИИ»

АКЦИОНЕРНОЕ ОБЩЕСТВО
«ВОЕННО-ИНЖЕНЕРНАЯ КОРПОРАЦИЯ»

Издается с сентября 1997 г.
Свидетельство о регистрации ПИ №77-3609 от 05.06.2000 г.
ISSN 1680-2780

Выходит 4 раза в год

Журнал включен в «Перечень ведущих периодических изданий» ВАК и систему РИНЦ

УДК 004.056

© Глухов А.П., Василенко В.В., Сидак А.А., Ададуров С.Е., Белова Е.И.
© Gluhov A., Vasilenko V., Sidak A., Adadurov S., Belova E.

ОПРЕДЕЛЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

DETERMINATION OF THE SECURITY LEVEL OF SIGNIFICATIVE OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE OF RAILWAY TRANSPORT

Аннотация. *В статье рассмотрены вопросы определения показателей безопасности функционирования объектов критической информационной инфраструктуры железнодорожного транспорта, моделирование их поведения в условиях неопределенности состояния и информационных воздействий для формирования области безопасного функционирования, оценки значимости показателей и определения уровней безопасности значимых объектов. Одним из возможных вариантов для исследования поведения показателей предложены параметрические модели на основе методов чувствительности систем для корпоративных информационных систем непрерывного действия и полумарковские модели для исследования временных характеристик систем реального времени с завершающим состоянием. Определение значимости показателей предложено проводить с использованием метода анализа иерархий, для реализации которого предложены иерархические структуры и определены их основные элементы.*

Abstract. *The article considers the issues of determining security indicators for the operation of railway transport critical information infrastructure objects, modeling their behavior in conditions of uncertainty and informational impacts to form a secure functioning area, assessing the significance of indicators and determining the security levels of significant objects. One of the possible options for research into the behavior of indicators has been proposed parametric models based on systems sensitivity methods for continuous corporate information systems and semi-Markov models for research into the time characteristics of real-time systems with a final state. It is proposed to determine the significance of indicators using the hierarchy analysis method, for the implementation of which hierarchical structures are proposed and their main elements are determined.*

Ключевые слова. *Критическая информационная инфраструктура, информационная безопасность, категорирование, критические процессы, метод анализа иерархий, объекты критической инфраструктуры, показатели безопасности функционирования.*

Key words. *Critical information infrastructure, information security, categorization, critical processes, hierarchy analysis method, critical infrastructure objects, operational security indicators.*

Информационная инфраструктура железнодорожного транспорта (ЖТ) – совокупность автоматизированных систем управления производственными и технологическими процессами и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, а также информационных систем и сетей связи (далее АИТС – автоматизированных, информационных и телекоммуникационных систем), предназначенных для решения задач управления перевозочным процессом, маркетингом, экономикой и финансами, инфраструктурой ЖТ, непроизводственной сферой, обеспечением движения поездов и безопасностью, имеющая свои особенности как объект обеспечения информационной безопасности [1,2].

Информационные системы (ИС), информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере транспорта, Федеральным законом № 187-ФЗ [3] отнесены к субъектам критической информационной инфраструктуры (КИИ) и подлежат категорированию.

При проведении категорирования объектов КИИ можно выделить следующие основные этапы [4]:

• определение критических процессов, т.е. выявление процессов, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка;

• формирование перечня АИТС ЖТ, подлежащих категорированию. Определение объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения критических процессов;

• категорирование объектов КИИ ЖТ, включающее в себя оценку возможных последствий в случае возникновения инцидентов информационной безопасности (ИБ) на объектах КИИ (определение значимых объектов КИИ).

В работах [4–7] предложены подходы и способы определения критических процессов, формирования перечня АИТС ЖТ, их категорирования и оценки значимости категорированных АИТС, рассмотрены вопросы определения уровней критичности информационных и программно-технических ресурсов корпоративных ИС ЖТ и систем железнодорожной автоматики и телемеханики (ЖАТ) для обеспечения безопасности функционирования АИТС ЖТ.

Однако, учитывая то, что основной целью создания систем безопасности объектов КИИ является обеспечение необходимого уровня безопасности АИТС ЖТ для исключения возникновения недопустимых негативных последствий, актуальной остается задача определение уровня безопасности значимых АИТС ЖТ, определяющего возможные ущербы в соответствии с перечнем показателей критериев значимости, определенных в [8].

Учитывая высокую сложность и комплексный характер проблемы анализа безопасности АИТС ЖТ, произвести оценку уровня безопасности только на основе одного какого-либо показателя АИТС затруднительно. Поэтому целесообразно рассматривать совокупность показателей, включающую как количественные, так и качественные характеристики, которые могут использоваться для формальной оценки безопасности АИТС. При этом, применяя классические подходы, используемые при оценивании больших систем, можно ориентироваться на три группы качественных и количественных системных показателей [9]:

• функциональные (характеризующие способность системы выполнять целевые задачи);

• оперативные;

• ресурсные (затраты на создание и функционирование АИТС ЖТ и их соотнесение с предотвращенным ущербом).

Данные показатели для конкретных АИТС ЖТ определяются в нормативных документах (национальных стандартах, технических заданиях, технических требованиях и других).

Так, например, в качестве показателей корпоративных ИС ЖТ могут выступать:

• количество автоматизированных рабочих мест, в том числе по типам;

• количество центров обработки данных (ЦОД);

• суммарная производительность ЦОД;

• количество центров хранения данных (ЦХД);

• суммарная емкость ЦХД;

• средняя пропускная способность локальных вычислительных сетей;

• средняя пропускная способность каналов внутрикорпоративного межсетевого взаимодействия;

• число шлюзов подключения к внешним информационно-телекоммуникационным сетям (ИТКС);

• суммарная пропускная способность каналов доступа к внешним ИТКС;

• и др.

Для систем диспетчерской централизации в соответствии с ГОСТ 33896-2016 [10] важным является выполнение требований по реализации функций телесигнализации и телеуправления, характеризуемых такими показателями, как:

• вероятность трансформации сигнала;

• вероятность потери информации в канале;

• вероятность ложного контрольного сообщения;

• время готовности системы к работе при включении питания;

• время реакции системы на управляющее воздействие оператора автоматизированного рабочего места;

• время от момента ввода команды до начала ее реализации объектом управления и другие.

В соответствии с ГОСТ 33358-2015 [11] показателями безопасности систем управления и обеспечения безопасности движения поездов являются:

• вероятность безопасной работы;

• вероятность опасного отказа;

• средняя наработка до опасного отказа;

• интенсивность опасных отказов;

• время возврата к безопасному состоянию;

• коэффициент безопасности;

• уровень полноты безопасности.

Безопасность АИТС ЖТ целесообразно определять посредством оценки ее показателей в условиях деструктивных информационных воздействий в процессе эксплуатации на протяжении всего жизненного цикла.

Безопасность характеризует допустимую эффективность функционирования АИТС ЖТ, т.е. нижние граничные значения показателей качества выполнения рассматриваемой системой заданного набора функций. Успешное выполнение АИТС ЖТ установленных функций и задач означает в итоге достижение заданных целей функционирования и во многом определяется устойчивостью выполнения АИТС своих задач, под которой будем понимать выполнение задач АИТС ЖТ с заданной надежностью в условиях имеющихся неопределенностей в параметрах модели поведения показателей системы и внешних воздействий. Устойчивость должна обеспечиваться как на этапе проектирования АИТС ЖТ, так и непосредственно в ходе ее эксплуатации (ситуационное управление реализуемостью задач) в условиях различного вида случайных и деструктивных воздействий и имеющихся неопределенностей в задании параметров качества АИТС ЖТ.

Для определения значений показателей АИТС ЖТ и поддержания их на уровне, обеспечивающем безопасное функционирование систем, требуется разработка моделей представления поведения показателей систем, на основе которых можно было бы делать обоснованные заключения о выполнении задач АИТС ЖТ.

Для оценки оперативных (временных) показате-

Глухов Александр Петрович *– доктор технических наук, доцент Петербургского государственного университета путей сообщения, тел. 8(916)528-47-14;*
Василенко Владимир Васильевич *– доктор технических наук, профессор, заместитель председателя, ООО «Центр безопасности информации», e-mail: v.vasilenko@cbi-info.ru;*
Сидак Алексей Александрович *– кандидат технических наук, старший научный сотрудник, заместитель председателя, ООО «Центр безопасности информации», e-mail:sidak@cbi-info.ru;*
Ададуров Сергей Евгеньевич *– доктор технических наук, профессор, заместитель директора, АО «Научно-исследовательский институт железнодорожного транспорта», 8(903)783-25-86;*
Белова Елена Ивановна *– аспирант кафедры «Информатика и информационная безопасность», ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I», тел. 8(921)124-85-71.*

Gluhov Alexandr *– doctor of technical science, PGUPS, tel. 8(916)528-47-14;*
Vasilenko Vladimir *– doctor of technical science, professor, deputy chairman, Information Security Center, e-mail: v.vasilenko@cbi-info.ru;*
Sidak Aleksey *– candidate of technical science, senior researcher, deputy chairman, Information Security Center, e-mail: sidak@cbi-info.ru;*
Adadurov Sergey *– doctor of technical science, professor, deputy director, JSC VNIIZhT, tel. 8(903)783-25-86;*
Belova Elena *– graduate student, PGUPS, tel. 8(921)124-85-71.*

лей АИТС и определения уровней безопасностей, прежде всего систем ЖАТ, систем управления и обеспечения безопасности движения поездов, некоторых типов корпоративных ИС ЖТ (обеспечивающих выполнение отдельных функций в реальном масштабе времени), представляется актуальным применение моделей оценивания вероятностно-временных характеристик выполнения функциональных задач, в качестве которых могут быть рассмотрены конечные полумарковские модели (цепи) непрерывных систем с завершающим (поглощающим) состоянием [12].

При этом в качестве наиболее полной характеристики устойчивости АИТС ЖТ можно рассматривать функцию распределения времени завершения цикла управления, в том числе и с учетом возможных воздействий на АИТС ЖТ. Поглощающее состояние системы определяется наступлением события завершения решения функциональных задач. Вероятность прибытия системы в поглощающее состояние в ходе реализации информационного процесса будет постоянно возрастать во времени, пока не достигнет величины, близкой к единице.

С помощью указанной характеристики можно решать как задачи анализа, так и задачи синтеза, в частности, управления процессом в АИТС для улучшения его оперативных характеристик и снижения рисков невыполнения АИТС ЖТ своих функциональных задач на заданном интервале времени.

В основу моделей исследования безопасности АИТС ЖТ как систем непрерывного действия могут быть положены модели конечномерных непрерывных многопараметрических систем, в условиях различного вида воздействий, заданными плотностью распределения вероятностей воздействий во времени [13] или моделью по типу эпидемий [14]. При этом динамика изменения показателей АИТС ЖТ определяется с учетом неопределенности значений параметров, входящих в модели поведения показателей и чувствительности показателей к вариациям этих параметров. Применение методов теории чувствительности для формирования частных функций влияния параметров на показатели АИТС ЖТ и нахождения предельных вариаций показателей по всем параметрам позволяет представить характер поведения показателя АИТС ЖТ, с учетом неопределенности в задании параметров модели и различных законах распределения времени воздействий, в виде соответствующих трубок траекторий (рис.1), а также учитывать (при наличии) взаимную корреляцию между вариациями параметров [15].

На рис. 1 приведен пример для нормального распределения информационных воздействий: $q(t)$ – показатель безопасного функционирования АИТС ЖТ; $FW_{sum}(t)$ – совокупная функция влияния параметров на показатель АИТС [15]; q_{mp} – требуемое для безопасного функционирования АИТС ЖТ значение показателя; $q(t)$–$FW_{sum}(t)$ и $q(t)$+$FW_{sum}(t)$ – соответственно, нижняя и верхняя граница трубки траекторий поведения показателя АИТС ЖТ.

Данный подход может быть положен в основу обоснования требований к показателям качества АИТС ЖТ как значимых объектов КИИ на этапе их проек-

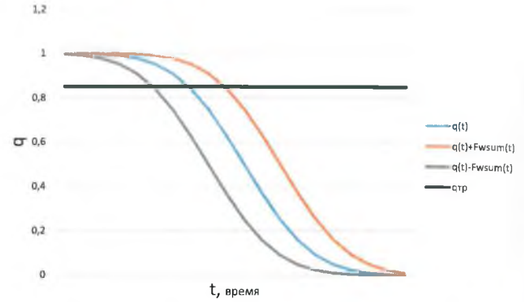

Рис. 1. Характер поведения (трубка траекторий) показателя безопасности АИТС ЖТ

тирования и в условиях динамичного совершенствования, а также контроля за выполнением требований по обеспечению их способности выполнить свои функциональные задачи и, соответственно, определения уровня безопасности АИТС ЖТ.

Показателем уровня безопасности АИТС ЖТ может выступать векторная совокупность частных показателей системы $Q_C=(q_1, q_2,...,q_n)$ либо один из критичных показателей системы (критический показатель $q_i = q_{кр}$, отражающий выполнение системой поставленной задачи).

В этом случае критерий безопасности будет иметь вид

$$Q_C \in \{Q_C\}_0, \qquad (1)$$

где $\{Q_C\}_0$ – область допустимых значений показателей системы, определяемых техническими требованиями к системе, и полученными в результате априорного экспертного анализа систем-аналогов, экспериментального и/или математического моделирования и

$$q_i > q_{i\,mp}, \qquad (2)$$

где $q_{i\,mp}$ – требуемое значение показателя, ниже которого система становится небезопасной в соответствии с перечнем показателей критериев значимости [8], который может определяться в нормативных правовых актах, технических требованиях на АИТС, национальных стандартах и других документах.

В рассматриваемом случае параметры $q_{i\,mp}$ представляют собой предельно допустимые граничные значения соответствующих показателей системы (нижние границы поведения показателей (трубки траекторий) АИТС в условиях неопределенности функционирования и различных законах распределения деструктивных воздействий).

Для целей анализа безопасности оценки степени деградации АИТС ЖТ целесообразно использовать нормированные показатели $z_i(k)$, которые вычисляются следующим образом [16]:

$$z_i(k) = a_i \frac{q_i(k) - q_{i\,mp}}{q_{i\,mp}}; \qquad (3)$$

для технических требований вида $q_i(k) \geq q_{i\,mp}$ или

$$z_i(k) = a_i \frac{q_{i\,mp} - q_i(k)}{q_{i\,mp}}; \qquad (4)$$

для технических требований вида $q_i(k) < q_{i\,mp}$.

Здесь $q_i(k)$ – текущее значение i-го показателя;

a_i – весовой коэффициент, характеризующий степень значимости i-го показателя для интегральной оценки уровня безопасности функционирования АИТС ЖТ в целом.

В результате можно построить пространственные модели АИТС ЖТ (см.рис. 2), в том числе и с учетом неопределенности факторов риска безопасности их функционирования.

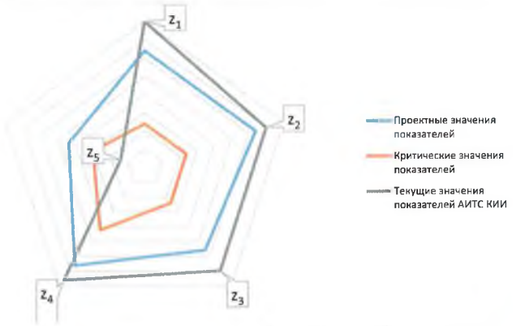

Рис. 2. Пространственный облик области безопасности АИТС ЖТ

Для реализации предложенного подхода одним из важных вопросов является определение весовых коэффициентов, характеризующих значимость показателей для оценки уровня безопасности функционирования АИТС ЖТ в целом.

Задача определения значимости показателей АИТС ЖТ может решаться экспертным путем с использованием метода анализа иерархий (МАИ) [5, 17] и формулироваться следующим образом.

Дано:

Множество показателей АИТС $\{(q)_i\}$, (i=1,2,…,N). Требуется:

- для каждого показателя из $\{q\}$, определить уровень его значимости r_i (в количественной шкале).

Определить подмножество показателей АИТС $\{(q^*)_i\} \subseteq \{(q)_i\}$,

для которых выполняется условие

$$r_i \geq r_{пр2},$$

где $r_{пр2}$ – пороговое значение значимости показателя АИТС, являющееся основанием для отнесения его к критическим и устанавливаемое экспертами.

Для построения конкретной иерархической структуры для определения значимости параметра АИТС в сфере ЖТ необходимо определить:

- цель функционирования АИТС;
- основные задачи, решаемые АИТС;
- определить показатели, невыполнение которых наносит ущерб при решении конкретной задачи АИТС.

Целью может быть обеспечение критичного процесса в рамках вида деятельности в сфере ЖТ. Перечень критических процессов определяется в рамках процедуры категорирования объектов КИИ ЖТ.

Основные задачи АИТС определяются в нормативных документах, регламентирующих вопросы создания конкретной АИТС, в частности, в техническом задании. Показатели АИТС также могут определяться национальными стандартами, отраслевыми стандартами и т.п.

Предлагаемая структура иерархии для определения значимости показателей для обеспечения безопасности АИТС ЖТ представлена на рис. 3. Её цель – с помощью применения МАИ определить инциденты ИБ, оказывающие наибольшее влияние на показатели безопасности АИТС ЖТ.

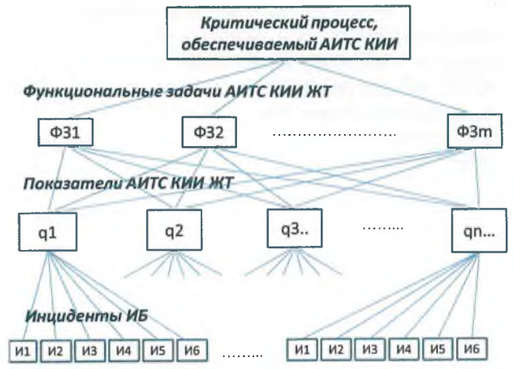

Рис. 3. Пространственный облик области безопасности АИТС ЖТ

В данной иерархии:

1-й уровень – процессы (определенные как критические) в рамках осуществления видов деятельности;

2-й уровень – задачи, решаемые АИТС;

3-й уровень – показатели, характеризующие безопасность АИТС ЖТ и заданные в технических требованиях;

4-й уровень – типы инцидентов ИБ: несанкционированный доступ, утечка данных, модификация (подмена) данных, отказ в обслуживании, нарушение функционирования (работоспособности) технических средств и систем, неправомерное использование вычислительных или иных активов [18].

В результате применения алгоритма МАИ на основе разработанной иерархии будет получен вектор приоритетов, каждый элемент которого (после нормирования) можно будет интерпретировать, как уровень влияния инцидента ИБ на конкретный показатель АИТС и последствия (для людей, территорий, экономики, государства), отраженные в значениях показателя критерия значимости объекта КИИ (для которого построена иерархия).

В дальнейшем, отработав алгоритм МАИ по всем показателям, можно будет на основе мажоритарного принципа определить значимость обобщенного показателя АИТС ЖТ.

При решении задачи отнесения экспертами показателей АИТС к критическим можно воспользоваться подходом, заключающимся в определении шкалы значимости показателей в терминах Н – «низкий ущерб», С – «средний ущерб», В – «высокий ущерб» и переопределении окончательного вектора приоритетов, что сделает его более пригодным для использования при определении наиболее значимых показателей АИТС.

Дополнительно следует отметить, что избежать субъективизма в определении весовых коэффициентов полностью невозможно, кроме того, эти «веса» суще-

ственно зависят от обстановки, в которой производится оценивание. Эти коэффициенты могут меняться от одного этапа разработки АИТС ЖТ к другому, зависеть от значений других показателей, которые также изменяются от этапа к этапу и т.д., и требуют периодического уточнения.

Тем не менее, знание «весовых коэффициентов» позволяет применять на практике различные подходы к оценке эффективности (в нашем случае, оценки безопасности) и выбору варианта построения (развития) АИТС ЖТ, например, методом построения обобщенных показателей как «взвешенной» суммы частных показателей, методом последовательных уступок, методом выделения главного показателя и др. [19].

Проведение работ по определению количественной оценки значимости показателей АИТС ЖТ возможно с использованием и доработкой апробированной нормативно-методической базы и специализированного программного комплекса, функционирующего в рамках программного модуля управления информационной безопасностью в составе автоматизированной системы управления информационной безопасности ЖТ.

Получаемые оценки уровней безопасности категорированных АИТС ЖТ позволят перейти к риск-ориентированному управлению, решению задач рационального формирования планов мероприятий по обеспечению безопасности значимых объектов КИИ ЖТ.

Литература

1. Глухов А.П., Ададуров С.Е., Диасамидзе С.В., Корниенко А.А., Сидак А.А. Особенности обеспечения информационной безопасности информационной инфраструктуры железнодорожной транспортной системы // Естественные и технические науки. – 2017. – № 11. – С. 258–267.

2. Глухов А.П. Особенности обеспечения информационной безопасности системы организации движения поездов // Транспорт Урала. – 2015. – № 3. – С. 32-40.

3. фраструктуры Российской Федерации: Федеральный закон Российской Федерации от 26 июля 2017 г. №187-ФЗ // Собр. Законодательства Рос. Федерации. – 2017. – № 31, ст. 4736.

4. Глухов А.П., Сидак А.А. Категорирование объектов критической информационной инфраструктуры железнодорожного транспорта// Естественные и технические науки. – 2018. – № 8. – С. 249 –255.

5. Сидак А.А. Применение метода анализа иерархий при определении критических процессов для категорирования объектов критической информационной инфраструктуры Российской Федерации // Информационные войны. – 2018. – № 2. – С. 79–82.

6. Сидак А.А., Корниенко А.А., Глухов А.П., Диасамидзе С.В. Категорирование и оценка значимости объектов критической информационной инфраструктуры железнодорожного транспорта // Двойные технологии. – 2019. – № 1. – С. 88 –93.

7. Глухов А.П., Василенко В.В., Сидак А.А. Определение уровней критичности информационных и программно-технических ресурсов объектов критической информационной инфраструктуры железнодорожного транспорта // Двойные технологии. – 2019. – № 2. – С. 83 –87.

8. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: Постановление Правительства Российской Федерации от 08.02.2018 № 127 //Собр. Законодательства Рос. Федерации. –2018. – № 8, ст. 1204.

9. Юсупов, Р.М. А.А. Мусаев Особенности оценивания эффективности информационных систем и технологий // Труды СПИИРАН, 2017, вып. № 2, С. 5–34.

10. ГОСТ 33896-2016 Системы диспетчерской централизации и диспетчерского контроля движения поездов. Требования безопасности и методы контроля. М: Стандартинформ, 2017.

11. ГОСТ 33358-2015 Безопасность функциональная. Системы управления и обеспечения безопасности движения поездов. Термины и определения. М: Стандартинформ, 2015.

12. Глухов А.П. Полумарковские модели оценивания вероятностно-временных характеристик выполнения функциональных задач автоматизированными системами управления критического применения // Естественные и технические науки. – 2015. – № 7. – С. 104–112.

13. Глухов А.П., Котяшев Н.Н., Лукин В.Л. Управление ресурсами проектируемых систем и комплексов критических приложений с заранее поставленными для них целями управления в условиях воздействий // Двойные технологии. – 2008. – № 1. – С. 46–55.

14. Глухов А.П., Котяшев Н.Н., Усков А.Ф. Модели оценки состояния непрерывных систем при воздействиях на них по типу эпидемий // Двойные технологии. – 2006. – № 4. – С. 61–67.

15. Глухов А.П., Котяшев Н.Н., Купцов А.В. Оценка чувствительности ресурсов и рисков применения систем критических приложений к влияющим факторам // Стратегическая стабильность. – 2007. – № 1. – С. 39–44.

16. Зиновьев П. А Анализ факторов и механизмов живучести в корпоративных информационных системах // Исследования по информатике: сб. науч. тр. / ИПИ АН РТ, Казань. – 2008. – вып. 12. – С. 3–30.

17. Саати Т. Принятие решений. Метод анализа иерархий. – М: "Радио и связь", 1993. – 312 с.

18. Аксененко Ю.И., Василенко В.В., Сидак А.А. Методологический подход к построению комплексных систем мониторинга и реагирования на инциденты информационной безопасности // Стратегическая стабильность. –2018. – № 1. – С. 64–67.

19. Дедков В. К. Принципы формирования критериев и показателей эффективности функционирования сложных технических систем// Надежность и качество сложных систем. – 2013. – № 4. – С.3–8.

Материал поступил в редакцию 16.10. 2019 г.

УДК 004.056

© Сидак А.А.
© Sidak A.

РЕШЕНИЕ ПРОБЛЕМ ЭКВИФИНАЛЬНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ПРИ СЦЕНАРНОМ ПОДХОДЕ МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

SOLVING THE PROBLEMS OF EQUIFINALITY OF OPERATIONAL SYSTEMS WITH A SCENARIO-BASED APPROACH TO MODELING INFORMATION SECURITY THREATS

Аннотация. *В статье рассмотрен новый подход к моделированию угроз безопасности информации в автоматизированных системах, направленный на повышение эквифинальности систем защиты информации и автоматизированных систем в целом. Подход основан на рассмотрении сценария реализации угрозы как цепочки событий безопасности информации, связанных с воздействием на активы автоматизированной системы. В качестве актива рассматриваются атомарные виды информации. Реализуемость угрозы определяется наличием векторов атаки и цепочки уязвимостей на всей трассе её реализации в автоматизированной системе (мулена безопасности). Указанный подход позволяет организовать итерационный процесс моделирования угроз безопасности информации в жизненном цикле автоматизированной системы, постоянно уточняя и обогащая его результаты новыми знаниями об автоматизированной системе, тактиках и техниках нарушителей. Результаты моделирования угроз будут служить исходными данными при определении функциональных требований безопасности и мер защиты информации в автоматизированных системах.*

Abstract. *The article describes a new approach to modeling information security threats in operational systems, aimed at improving the equifinality of information security systems and automated systems in General. The approach is based on considering the threat implementation scenario as a chain of information security events related to the impact on an operational system asset. Atomic types of information are considered as an asset. The feasibility of the threat is determined by the presence of attack vectors and the chain of vulnerabilities along the entire path of its implementation in the operational system (security mulen). This approach allows to organize an iterative process of information security threats modeling in the life cycle of an operational system, refining and enriching its results with new knowledge about the operational system, tactics and techniques of attacker. The results of threat modeling will serve as input data for determining functional security requirements and information security controls in operational systems.*

Ключевые слова. *Угроза безопасности информации, моделирование угроз, модель угроз, сценарный подход, сценарий, событие безопасности, автоматизированная система, эквифинальность, уязвимость, мулен безопасности, тактика, техника, нарушитель, вектор атаки, функциональное требование безопасности, мониторинг, инцидент.*

Key words. *Information security threat, threat modeling, threat model, scenario approach, scenario, security event, operational system, equifinality, vulnerability, security moulin, tactic, technique, attacker, attack vector, functional security requirement, monitoring, incident.*

В условиях потребностей цифровой трансформации необходимо обеспечить возможность развития автоматизированных систем (АС), то есть повысить их эквифинальность. Эквифинальность АС определена в работе [1] как свойство АС, характеризующее предельные возможности АС (количество обрабатываемой информации, поддерживаемых видов информации, реализуемых информационных сервисов, поддерживаемых пользователей, структурных элементов, типов взаимодействий с иными системами) при данном уровне применяемых информационных технологий (ИТ), капиталовложений и эксплуатации.

Развитие АС сопровождается применением большего числа изделий ИТ, новых информационных сервисов, связанных с конфиденциальностью, целостностью и доступностью, а значит, уязвимых для компьютерных атак и подверженных инцидентам информационной безопасности (ИБ).

Защита информации (ЗИ) в АС предполагает принятие мер ЗИ, направленных на нейтрализацию (блокирование) угроз безопасности информации (БИ).

Область угроз БИ расширяется, и постоянно появляются новые угрозы БИ, источники угроз БИ и векторы атак. Защита от угроз БИ требует, чтобы операторы АС знали о таких угрозах, их источниках и уровнях опасности. Такие знания появляются в процессе моделирования угроз БИ.

Предельные возможности (эквифинальность) си-

Сидак Алексей Александрович *– кандидат технических наук, старший научный сотрудник, заместитель председателя, ООО «Центр безопасности информации», e-mail:sidak@cbi-info.ru.*

Sidak Aleksey *– candidate of technical science, senior researcher, deputy chairman, Information Security Center, e-mail: sidak@cbi-info.ru.*

стемы ЗИ АС характеризуются количеством угроз БИ, для которых может быть обеспечена их нейтрализация (блокирование).

Таким образом, чтобы сформировать функциональные требования безопасности (ФТБ) АС, которым должны отвечать меры ЗИ в рамках системы ЗИ АС, необходимо составить наиболее полную модель угроз БИ [2-4].

1. Парадигма моделирования угроз БИ

Согласно национальному стандарту ГОСТ Р 50922 [5], угроза БИ – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения БИ.

С исследовательской точки зрения угрозу БИ целесообразно рассматривать как возможное событие безопасности или цепочку событий безопасности, приводящих к ущербу.

Угрозу БИ можно охарактеризовать источником угрозы, который осуществляет действия в рамках своих возможностей. Эти действия приводят к наступлению событий.

Действия источника угрозы воздействуют на конкретный компонент АС. Возможности нарушителя характеризуются его потенциалом и дефектами, слабостями (уязвимостями) компонента.

Непосредственно воздействие осуществляется на информацию:

• как часть компонента АС (программное обеспечение, служебные базы данных, в том числе настройки);

• контролируемую или преобразуемую компонентом АС информацию предметной области в соответствии с предназначением АС.

Результат реализации угрозы БИ – ущерб информационным сервисам АС, которые реализуются компонентами АС. Таким образом, угрозы БИ оказывают отрицательное влияние на эквифинальность АС [1].

Угрозы БИ также оказывают влияние (в совокупности с иными факторами) на возникновение и реализацию иных типов (уровней) угроз:

• угрозы бизнес-процессам оператора АС, которые поддерживаются информационными сервисами АС;

• угрозы возникновения негативных последствий в области деятельности оператора.

Чтобы угроза БИ могла быть реализована, должны существовать точка доступа или канал (подключение к Интернет, интерфейс для подключения съемного машинного носителя и т.п.), то есть так называемый вектор атаки [6,7].

Описания одного только вектора атаки для разработки мер ЗИ явно недостаточно. Поэтому при моделировании угрозы БИ, как правило, составляют ее сценарий. Сценарий угрозы БИ (см. рис. 1) можно представить в виде набора упорядоченных по времени событий (событий безопасности), вызванных действиями источника угрозы БИ (нарушителя).

При этом в описание сценария угроз БИ нецелесообразно включать непосредственные действия нарушителя (например, на уровне тактик, техник и процедур) [7, 8], так как к одному событию на практике могут приводить разные совокупности действий нарушителя. Соответственно техническая детализация сценария, с одной стороны, не будет полной, а с другой стороны, меры защиты, направление на противостояние сценарию могут быть необоснованно ограничивающими. Таким образом, это будет негативно отражаться как на эффективности и эквифинальности системы ЗИ АС, так и АС в целом.

Задание сценария на уровне цепочки событий не будет давать нарушителю (при ознакомлении) понимание, что защита реализована против конкретных тактик, техник и процедур. Также это потребует от оператора АС на этапах проектирования, внедрения и эксплуатации АС рассматривать конкретные тактики, техники и процедуры (информация о них постоянно пополняется) [7, 8], то есть постоянно итерационно продолжать моделировать угрозы БИ.

Задание сценариев на уровне цепочки событий будет предполагать эффективное использование национального стандарта ГОСТ Р «Защита информации. Регистрация событий безопасности. Требования к составу регистрируемой информации» (проект стандарта разработан в рамках рабочей группы технического комитета по стандартизации «Защита информации» ТК 362), который определил требования к составу и содержанию регистрируемой информации для различных типов событий безопасности. На этапе проектирования данный стандарт будет определять выбор изделий ИТ, регистрирующих соответствующие типы событий безопасности и информацию о них.

Сценарии угроз БИ могут быть представлены в вербальной, графической формах или древовидной структуре. Детализация сценария угрозы БИ, а также рассмотрение конкретных действий нарушителей, приводящих к событиям сценария целесообразно осуществлять при проектировании и разработке АС. Особенно важным является постоянное уточнение сценария угрозы в процессе эксплуатации АС.

При этом реализуемость угрозы БИ определяется наличием векторов атаки и уязвимостей на всей трассе её реализации в АС.

Исходя из этого необходимым условием реализуемости угрозы является наличие цепочки уязвимостей, для обозначения которой введем термин «мулен безопасности» (по аналогии с муленами – узкими трубчатыми отверстиями в ледниках, образованными талыми водами, которые могут пробивать сотни метров льда и достигать его основания) (см. рис. 2).

Рис. 1. Представление сценария угрозы БИ в виде цепочки событий

Рис. 2. Цепочка уязвимостей (мулен безопасности)

Для обеспечения лучшего понимания угроз БИ необходимо моделирование угроз БИ не завершать только их непосредственным описанием, но и сопоставлять угрозы БИ с соответствующими мерами ЗИ (возможно изложенными в достаточно общем виде). Это позволит на последующих этапах создания и эксплуатации АС обеспечить применение итеративного процесса моделирования угроз БИ, уточнения ФТБ и принятия соответствующих мер ЗИ в АС.

2. Методическое регулирование моделирования угроз БИ

До настоящего времени в стране не существовало единого методического обеспечения моделирования угроз БИ. Имелись отдельные методические документы для областей обеспечения безопасности персональных данных, ключевых систем информационной инфраструктуры. Также де-факто активно применялся проект методического документа ФСТЭК России 2015 г., размещенный на сайте Федеральной службы [9].

В 2020 г. при участии экспертов ведущих организаций в области ЗИ, включая Центр безопасности информации, ФСТЭК России подготовлен проект нового методического документа «Методика моделирования угроз безопасности информации». Указанный проект документа был анонсирован и доложен представителями ФСТЭК России на X Конференции «Актуальные вопросы защиты информации» (12 февраля 2020 г.) в рамках Международного форума «Технологии безопасности» (ТБ Форум).

Результаты анализа материалов проекта документа показывают следующее:

• документ реализует сценарный подход к моделированию угроз БИ;

• документ направлен на моделирование угроз БИ не только для отдельных АС, но и для информационной инфраструктуры (ИИ) в целом, как совокупности взаимодействующих систем и сетей;

• документ ориентирован на применение комбинации методов моделирования угроз БИ: метод, сфокусированный на активы (asset-) и ущерб (impact-), и метод, сфокусированный на нарушителя (attacker-) и угрозу (threat-);

• предполагается все угрозы БИ, для которых имеется реализуемый сценарий, рассматривать как актуальные;

• предусмотрена градация актуальных угроз БИ по уровню их опасности с целью приоритезации применения мер ЗИ.

В целом проект методического документа ФСТЭК России «Методика моделирования угроз безопасности информации» предусматривает следующую процедуру моделирования угроз БИ:

• оценку возможностей нарушителей;

• определение информационных ресурсов (ИР), подверженных угрозам БИ;

• определение угроз БИ, как возможные воздействия на ИР, которые приводят к ущербу для этих ресурсов;

• определение сценариев реализации угроз БИ;

• оценку уровня опасности угрозы БИ.

2.1. *Оценка возможностей нарушителя*

Согласно подходу ФСТЭК России последовательность оценки возможностей нарушителя следующая:

• определение целей нарушителя и видов нарушителей;

• определение потенциала нарушителя, как уровня его возможностей;

• определение возможностей нарушителей по реализации угроз БИ.

Примеры целей нарушителя:

• нанесение ущерба государству, отдельным его сферам (областям) деятельности или секторам экономики;

• совершение террористических актов, дестабилизация общества;

• получение конкурентных преимуществ;

• мошенничество, кража.

Рассматриваемые виды нарушителей:

• специальные службы иностранных государств;

• террористические, экстремистские организации;

• преступные группы;

• конкурирующие организации;

• отдельные физические лица (хакеры);

• пользователи;
• и др.

Исходя из целей и видов нарушителей по таблице определяется потенциал нарушителей (высокий, средний, базовый повышенный или базовый).

Таким образом, определяется потенциал нарушителей, которым необходимо противостоять в АС, например, «базовый повышенный» (не выше). На повышение потенциала нарушителя, которому необходимо противостоять, могут оказывать влияние сведения о его мотивации.

Каждое значение потенциала нарушителя в проекте методического документа ФСТЭК России сопоставлено с его возможностями.

Например, потенциал «базовый повышенный» предполагает наличие у нарушителя следующих возможностей:

• реализации целевых угроз безопасности информации (компьютерных атак);
• хорошего владения средствами (инструментами) для реализации угроз БИ и использования уязвимостей;
• наличия навыков самостоятельного планирования и реализации угроз БИ;
• обладания практическими знаниями о функционировании систем и сетей, операционных систем (ОС), а также о защитных механизмах, применяемых в программном обеспечении (ПО), программно-аппаратных средствах;
• и др.

2.2. *Определение информационных ресурсов*

Согласно подходу ФСТЭК России процесс моделирования угроз БИ должен охватывать все ИР, составляющие ИИ обладателя информации и (или) оператора, воздействие на которые при реализации (возникновении) угроз БИ может привести к недопустимым негативным последствиям.

Можно выделить следующие типы ИР, которые необходимо учитывать [2, 3, 10]:

• аппаратное обеспечение (средства вычислительной техники, в том числе мобильные устройства, серверы, встраиваемое ПО, интегральные микросхемы, интерфейсы);
• системное ПО (ОС и иное ПО с системными привилегиями, системы управления базами данных);
• прикладное ПО (клиент-серверное ПО, web-приложения, браузеры, иное ПО);
• телекоммуникационное оборудование (маршрутизаторы, коммутаторы, мультиплексоры, концентраторы, сетевое оборудование, коммутационные элементы, сетевые интерфейсы, сетевое ПО, телекоммуникационные сервисы);
• средства виртуальной инфраструктуры (гипервизоры, виртуальные машины, контейнеры, серверы виртуализации, системы управления виртуализацией, виртуальными каналами связи и др.)
• машинные носители информации (магнитные, электронные, оптические, в том числе съемные, а также системы хранения данных);
• бумажные носители информации (распечатанные выходные данные, документация на систему);
• средства отображения информации (дисплеи, мониторы, панели, видеопроекторы);
• средства вывода информации (принтеры, плоттеры, многофункциональные устройства, средства вывода аудиоинформации);
• средства ввода информации (клавиатура, мышь, сканеры, микрофоны, видеокамеры);
• средства ЗИ, средства обеспечения безопасности ИТ, средства управления событиями ИБ, средства управления инцидентами ИБ;
• информацию, данные, электронные документы (объекты файловой системы, базы данных и др.);
• служебные данные (конфигурационная информация, регистрационная информация, информация управления, статистическая информация);
• пользователей (учетные записи, аутентификационная информация, сеансы, психофизические свойства пользователей);
• средства обеспечения функционирования (технические средства электроснабжения, кондиционирования, заземления);
• средства генерирования надежных меток времени и синхронизации системного времени.

В развитие подхода ФСТЭК России представляется целесообразным применение сфокусированного на данные (data) подхода, предложенного в работе [10]. Он является более адекватным на этапе создания АС и нацелен на финальные активы (данные) вне зависимости от их расположения.

2.3. *Определение угроз БИ*

В подходе ФСТЭК России угрозы БИ определяются как возможные воздействия по отношению к конкретному ИР, которые приводят к ущербу (недопустимым последствиям).

Примерами недопустимых последствий являются следующие:

• отказ в обслуживании;
• несанкционированный доступ;
• утечка (нарушение конфиденциальности) информации;
• модификация (подмена) информации;
• несанкционированное использование вычислительных ресурсов;
• нарушение функционирования (работоспособности).

2.4. *Определение сценариев реализации угроз БИ*

Для того, чтобы определить актуальность конкретной угрозы БИ, предполагается разработка сценария ее реализации.

Сценарий реализации угрозы БИ в проекте методического документа предполагается описывать в виде действий нарушителей в терминах тактик (задач, решаемых нарушителем), техник (действий, осуществляемых нарушителем для решения своих задач) по аналогии с современными международными подходами, рассмотренными в работе [7]. В качестве тактик рассматриваются: сбор информации об АС; получение первоначального доступа; внедрение и использование вредоносного ПО; сохранение полученного доступа к компонентам АС; управление внедренным ПО и (или) компонентами; повышение привилегий по доступу; обеспечение скрытности действий нарушителя; распространение возможностей нарушителя по доступу на смежные компоненты систем и сетей; сбор и вывод из АС интересующей нарушителя информации; воздействие на компоненты АС, приводящее к недопустимым последствиям.

Сценарий реализации угрозы БИ строится с учетом ранее определенных возможностей нарушителя (в соответствии с потенциалом). Если сценарий осуществим, то угроза БИ для АС или ИИ в целом считается актуальной.

Разработка сценариев для множества угроз БИ для АС представляется достаточно трудоемким процессом. Чтобы ускорить эту работу и повысить качество результатов ФСТЭК России планируется переработать банк данных угроз безопасности информации (https://bdu.fstec.ru/threat (БДУ ФСТЭК России)). При включении в него описания типовых угроз БИ необходимо соотнести описания сценариев угроз с потенциалом нарушителя, необходимым для их осуществления.

Для этого предлагается определить значимые характеристики нарушителя, например, следующие: категория нарушителя, компетентность, оснащенность, знания об объекте воздействия, вид доступа, время доступа и др. Для указанных характеристик определить смысловые значения, например, для характеристики «категория нарушителя» значения «внешний» и «внутренний». Экспертным способом сопоставить смысловым значениям числовые, например, «внутренний» – 0, внешний – 3. Итоговая таблица значений характеристик нарушителя может выглядеть по форме аналогично таблице определения требуемого потенциала нарушителя для использования уязвимости, приведенной в ГОСТ Р ИСО/МЭК 18045 [11].

Диапазоны суммарных значений характеристик нарушителя также аналогично по форме ГОСТ Р ИСО/МЭК 18045 [11] можно сопоставить с потенциалами нарушителей и представить в виде таблицы.

Далее указанными таблицами можно будет пользоваться для определения потенциала нарушителя, требуемого для осуществления сценария угрозы БИ, при её каталогизации в обновленном БДУ ФСТЭК России.

В последствии, оценивая актуальность угрозы БИ для АС или ИИ, достаточно будет сравнить потенциал нарушителя, которому необходимо противостоять, с потенциалом нарушителя, требуемым для реализации сценария угрозы БИ. Это позволит оценить реализуемость сценария и актуальность угрозы БИ.

2.5. *Определение уровня опасности угрозы БИ*

Реализация мер защиты в АС по отношению ко всем актуальным угрозам БИ, то есть угрозам, для которых есть реализуемый сценарий, может быть труднореализуемой с технической или финансовой точки зрения.

Поэтому целесообразно определить приоритеты противостояния в АС угрозам БИ.

В проекте методического документа ФСТЭК России такая приоритезация предусмотрена на основании уровня опасности угрозы БИ (низкий/ средний/ высокий).

В качестве факторов опасности угрозы, в частности, рассматриваются:

• тип доступа (удаленный/ локальный/ физический);
• сложность реализации угрозы БИ;
• количество затронутых компонентов или пользователей;
• последствия от реализации угрозы БИ.

Если угроза БИ имеет несколько сценариев реализации, то для определения ее опасности может применяться мажоритарный принцип, исходя из наихудшего сценария.

В целом, как ожидается, принятие нового методического документа ФСТЭК России по моделированию угроз будет, несомненно, большим шагом вперед в отечественной практике моделирования угроз БИ для АС. При этом с целью снижения рисков и получения положительного эффекта, с точки зрения эквифинальности АС, представляется целесообразным развить содержание указанного документа в части, предложенной в настоящей статье парадигмы:

• рассмотрения ИР в виде атомарных видов информации вне зависимости от привязки к программно-аппаратным компонентам;
• описания сценария угрозы БИ в виде цепочки событий безопасности;
• каталогизации угроз БИ и сценариев угроз в банке данных с определением потенциала и возможностей нарушителя, необходимых для осуществления сценария;
• систематической итерационной детализации сценария угрозы БИ на этапах проектирования, внедрения и эксплуатации АС в части рассмотрения конкретных техник, тактик и процедур, применяемых нарушителями;
• применения в составе системы ЗИ АС изделий ИТ, позволяющих регистрировать события безопасности, включенные в сценарии угроз БИ (см. рис. 3);

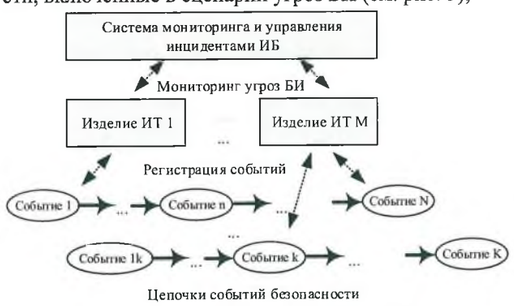

Рис. 3. Мониторинг угроз БИ в АС

• организации мониторинга реализации угроз БИ в части контролируемых событий безопасности, включенных в сценарий (см. рис. 3);
• управления инцидентами ИБ, основанного на реагировании на реализацию угроз БИ (см. рис. 3).

Для реализации мониторинга ИБ и управления инцидентами ИБ в АС могут быть использованы средства автоматизации типа NeuroDAT [12].

Литература
1. Сидак А.А. Сквозная реализация функциональных требований безопасности за счет обеспечения специальных свойств автоматизированных систем. Показатели эквифинальности// Стратегическая стабильность. – № 2. – 2019. – С. 62–65.
2. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», зарегистрирован в Минюсте России 31.05.2013 № 28608 // СПС КонсультантПлюс.
3. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», зарегистрирован в Минюсте России 26.03.2018 № 50524 // СПС КонсультантПлюс.
4. Сидак А.А. Обоснование требований по защите информации в автоматизированных системах // Стратегическая стабильность. – № 4. – 2009. – С. 7–9.
5. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. – М.: Стандартинформ, 2008.
6. Draft NIST Special Publication NIST 800-154 Guide to Data-Centric System Threat Modeling, March 2016 // National Institute Standards and Technology: [сайт]. URL: https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf (дата обращения: 19.02.2020).
7. Аксененко Ю.Й, Сидак А.А. Современные подходы к моделированию угроз безопасности информации. Источники информации об угрозах безопасности информации (Часть 1) // Центр безопасности информации, 2006-2019: [сайт]. URL: http://www.cbi-info.ru/groups/page-1306.htm (дата обращения: 19.02.2020).
8. Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, Cody B. Thomas MITRE ATT&CK™: Design and Philosophy, July 2018// MITRE ATT&CK™: [сайт]. URL: https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf (дата обращения: 20.02.2020).
9. Методический документ ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» (проект)// ФСТЭК России: [сайт]. URL: https://fstec.ru/component/attachments/download/812 (дата обращения: 21.02.2020).
10. Сидак А.А. Подход к формированию функциональных требований безопасности автоматизированных систем, базирующийся на выделении и систематизации атомарных видов защищаемой информации// Информационные войны. – 2019. – № 4. – С. 90–92.
11. ГОСТ Р ИСО/МЭК 18045 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. М.: Стандартинформ, 2014.
12. Аксененко Ю.И., Василенко В.В., Сидак А.А. Методологический подход к построению комплексных систем мониторинга и реагирования на инциденты информационной безопасности // Стратегическая стабильность. – 2018. – № 1. – С. 64–67.

Материал поступил в редакцию 06.03. 2020г.

УДК 629.7.017

© Зорин Э.Ф., Бубенщиков Ю.Н. Рыжов Б.С., Гвоздева Г.А.
© Zorin E., Bubenshchikov Y., Ryzhov B., Gvozdeva G.

ЭКСПЕРТНО-АНАЛИТИЧЕСКИЙ СПОСОБ ОЦЕНКИ ЗАЩИЩЁННОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ, ФУНКЦИОНИРУЮЩИХ В УСЛОВИЯХ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ ПОТЕНЦИАЛЬНОГО НАРУШИТЕЛЯ

EXPERT AND ANALYTICAL WAY OF THE ASSESSMENT OF SECURITY BJECTS OF INFORMATION INFRASTRUCTURE OF THE AUTOMATED SYSTEM OF THE SPECIAL PURPOSE, FUNCTIONING IN THE CONDITIONS OF INFORMATION AND TECHNICAL INFLUENCES OF THE POTENTIAL INTRUDER

Аннотация. *Настоящая статья посвящена решению одной из важных задач – разработке методического обеспечения информационной безопасности объектов информационной инфраструктуры автоматизированной системы специального назначения (АС СН), функционирующих в условиях деструктивных информационно-технических воздействий (ИТВ) потенциального нарушителя, в том числе и возможных деструктивных воздействий его беспилотных летательных аппаратов (БПЛА). Внедрение методического обеспечения защищенности объектов АС СН в процесс управления информационной безопасностью информационной инфраструктура АС СН обеспечивает формирование и своевременное принятие эффективных мер по защите информационно-телекоммуникационных структур АС СН и достижению требуемого уровня устойчивости их функционирования в условиях возможных деструктивных ИТВ потенциального нарушителя [1].*

Abstract. *The present article is devoted to the solution of one of important tasks - development of methodical ensuring information security of objects of information infrastructure of the automated system of a special purpose (AS SP), functioning in the conditions of destructive information and technical influences (ITI) of the potential intruder, including possible destructive influences of his pilotless aircraft (PA). Introduction of methodical ensuring security of objects AS SP in management of information security information AS SP provides formation and timely acceptance of effective measures on protection of information and telecommunication structures AS SP and to achievement of demanded level of stability of their functioning in the conditions of possible destructive ITV of the potential intruder [1].*

Ключевые слова. *Оценка защищенности объектов, информационно-техническое воздействие, информационная безопасность, вероятность устойчивого функционирования, программно-инструментальные средства сканирования.*

Key words. *Assessment of security of objects, information and technical influence, information security, probability of steady functioning, scanning program tools.*

Актуальность решаемой задачи

Эффективность функционирования объектов информационной инфраструктуры АС СН в условиях деструктивных ИТВ потенциального нарушителя во многом определяется их защищенностью при выполнении ими функций сбора, обработки, представления данных и передачи информации.

Использование в средствах информатизации объектов информационной инфраструктуры АС СН стандартных средств защиты данных и большого разнообразия зарубежных информационных технологий по защите информации не гарантируют требуемый уровень защищенности этих объектов, функционирующих в условиях возможных деструктивных ИТВ потенциального нарушителя.

Несовершенство средств защиты объектов информационной инфраструктуры АС СН приводит к тому, что в реальных условиях неизвестные ИТВ потенциального нарушителя, преодолевая рубежи защиты объектов информационной инфраструктуры АС СН, оказывают деструктивные воздействия на эффективность их функционирования.

Зорин Эдуард Федорович *– кандидат технических наук, старший научный сотрудник, ведущий научный сотрудник, ФГБУ «4 ЦНИИ» Минобороны России, тел. 8(495) 544-26-24;*
Бубенщиков Юрий Николаевич *– кандидат технических наук, старший научный сотрудник, старший научный сотрудник, ФГБУ «4 ЦНИИ» Минобороны России;*
Рыжов Борис Сергеевич *– кандидат технических наук, доцент, начальник отдела, ФГБУ «4 ЦНИИ» Минобороны России;*
Гвоздева Галина Алексеевна *– научный сотрудник, ФГБУ «4 ЦНИИ» Минобороны России.*

Zorin Eduard *– candidate of technical sciences, senior researcher, leading researcher, FSBI «4 CRI» of the Ministry of Defense of Russia, tel. 8 (495) 544-26-24;*
Zorin Eduard *– candidate of technical sciences, senior researcher, senior researcher, FSBI «4 CRI» of the Ministry of Defense of Russia;*
Ryzhov Boris *– candidate of technical sciences, associate professor, head of department, FSBI «4 CRI» of the Ministry of Defense of Russia;*
Gvozdeva Galina *– researcher, FSBI «4 CRI» of the Ministry of Defense of Russia.*