УДК 004.056.53

МЕТОД ЗАЩИТЫ ДАННЫХ ОТ ВОЗДЕЙСТВИЯ ФАКТОРОВ, ОПРЕДЕЛЯЮЩИХ УГРОЗЫ ИХ РАЗРУШЕНИЯ

В. А. Журавлев, К. А. Соседко

В статье рассмотрены механизмы обеспечения информационной безопасности эргатических систем. Совершенствование цифровых технологий предполагает развитие средств обработки информации как в реализации созидательных процессов, так и в возможностях построения средств разрушения. Целью статьи является анализ механизмов защиты цифровой информации на основании объективного выявления угроз и выбора контрмер, эффективных для смягчения деструктивных воздействий внешних факторов (TARA). На основе совместного применения метода TARA и PDCA-модели рассмотрены механизмы создания системы менеджмента информационной безопасности, повышающие эффективность обеспечения защиты передаваемых сообщений. Показано, что применение метода TARA в сочетании с PDCA-моделью является перспективным подходом к обеспечению информационной безопасности и защите информационных активов.

Ключевые слова: *информационная безопасность, защита данных, выявление угроз, выбор контрмер, модель PDCA, метод TARA.*

Введение

В современном цифровом обществе в условиях непрерывно обновляющегося потока данных информационные технологии оказывают значительное влияние на формирование систем обеспечения безопасности в ракетно-космической отрасли. Развитие средств защиты от воздействия факторов, угрожающих разрушением баз данных, во многом определяется уровнем научного, экономического и военного потенциалов производственных комплексов.

В ракетно-космической отрасли ускорение интенсивности потоков передаваемой информации, масштабное внедрение облачных технологий, развитие интернета вещей, цифровизация производственных процессов создают предпосылки для внедрения инноваций в расширение технологических приемов создания и серийного выпуска средств защиты информационных активов. Для обеспечения надежности передачи сообщений ставится задача системной реализации методологических возможностей поддержания информационной безопасности (ИБ) трафика.

Информационная безопасность

Целью системы ИБ является анализ уязвимостей, общих для средств управления технологическим процессом на различных предприятиях. Разнообразие производств определило необходимость ввести в рассмотрение сущность, инвариантную к их специфике. В качестве такой сущности предлагается ИБ. Особенностью ее рассмотрения в качестве ценного актива является необходимость сохранения ее дееспособности на всем периоде существования.

Защита информационных активов посредством определения, достижения, поддержания и улучшения ИБ имеет важное значение для обеспечения намеченных организацией целей, а также для сохранения высокого уровня соответствия законодательным нормам [1].

Система менеджмента информационной безопасности

Высокий уровень ИБ достигается посредством внедрения соответствующих мер, определенных в ходе выбранного процесса менеджмента рисков и управляемых с помощью системы менеджмента ИБ (СМИБ).

СМИБ представляет собой скоординированные действия, направленные на внедрение соответствующих мер обеспечения ИБ, обработку недопустимых рисков в области ИБ, а также действия по управлению организацией, контролю и совершенствованию ее соответствующих структур [2].

На предприятии АО «Корпорация «ВНИИЭМ» СМИБ сертифицирована Британским институтом стандартов (BSI) на соответствие требованиям международного стандарта ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements, что свидетельствует о высоком уровне ИБ [3].

Построение СМИБ основывается на создании модели PDCA – кругового цикла Деминга – Шухарта, в основе которого лежит последовательное прохождение четырех этапов (рис. 1):

1. Plan (планирование) – фаза создания СМИБ, создание перечня активов, оценки рисков и выбора мер.
2. Do (действие) – этап реализации и внедрения соответствующих мер.
3. Check (проверка) – фаза оценки эффективности и производительности СМИБ. Обычно выполняется внутренними аудиторами.
4. Act (улучшения) – выполнение превентивных и корректирующих действий [4].

Рис. 1. Круговой цикл Деминга – Шухарта

На базе PDCA выстраиваются службы и процессы ИБ с целью повышения уровня качества управления ИБ, а СМИБ является стратегией построения и перестроения службы ИБ с начала внедрения процессов по всему предприятию, что является преимуществами модели PDCA. Однако концепция PDCA не является единственным инструментом для управления ИБ и подходит для общего планирования и контроля процессов ИБ, тогда как для более детального анализа и принятия решений по защите информации требуется использование дополнительных методов, таких как TARA.

Метод TARA

Между принципом PDCA, реализующимся в СМИБ, и TARA можно проследить взаимосвязи: этапы TARA имеют прямое соответствие этапам PDCA. Данное соответствие показано в табл. 1.

Методология TARA включает в себя три мероприятия:

– анализ восприимчивости к угрозам разрушения данных (АВР);

– анализ устранения рисков разрушения данных (АУР);

– разработку данных и инструментов (РДИ).

На этапе первого мероприятия АВР оцениваются детали архитектуры системы и технологии для выявления и выбора репрезентативного набора уязвимостей. Результатом этого этапа является матрица уязвимостей, которая используется на следующем этапе.

На этапе второго мероприятия АУР происходит оценка и выбор контрмер из каталога для устранения уязвимостей, описанных в матрице уязвимостей. На данном этапе предоставляются рекомендации TARA, определяющие контрмеры, которые обеспечивают оптимизированный коллективный ответ на список уязвимостей.

Таблица 1

Соответствие этапов PDCA и TARA

ID этапа	Наименование этапов PDCA (СМИБ)	Этапы TARA
P	планирование	Разработка кибернетической модели системы
D	действие	Определение вероятных векторов атак
		Оценка рисков
C	проверка	Определение возможных мер по смягчению последствий
		Оценка полезности и стоимости мер по смягчению последствий
A	улучшение	Выбор мер по смягчению последствий
		Определение приоритетности информационных потребностей
		Выявление и оценка внешних источников данных
		Обновление данных каталога

На заключительном этапе РДИ разрабатывается содержимое каталога, обеспечивается внутренняя согласованность данных каталога и отражается постоянно меняющаяся информация об угрозах и контрмерах [5].

Эти мероприятия поддерживают три рабочих процесса: оценка TARA, разработка каталога, разработка набора инструментов.

Для наглядного представления способа организации ИБ с использованием метода TARA была построена функциональная модель IDEF0 в соответствии с Р 50.1.028-2001 (рис. 2).

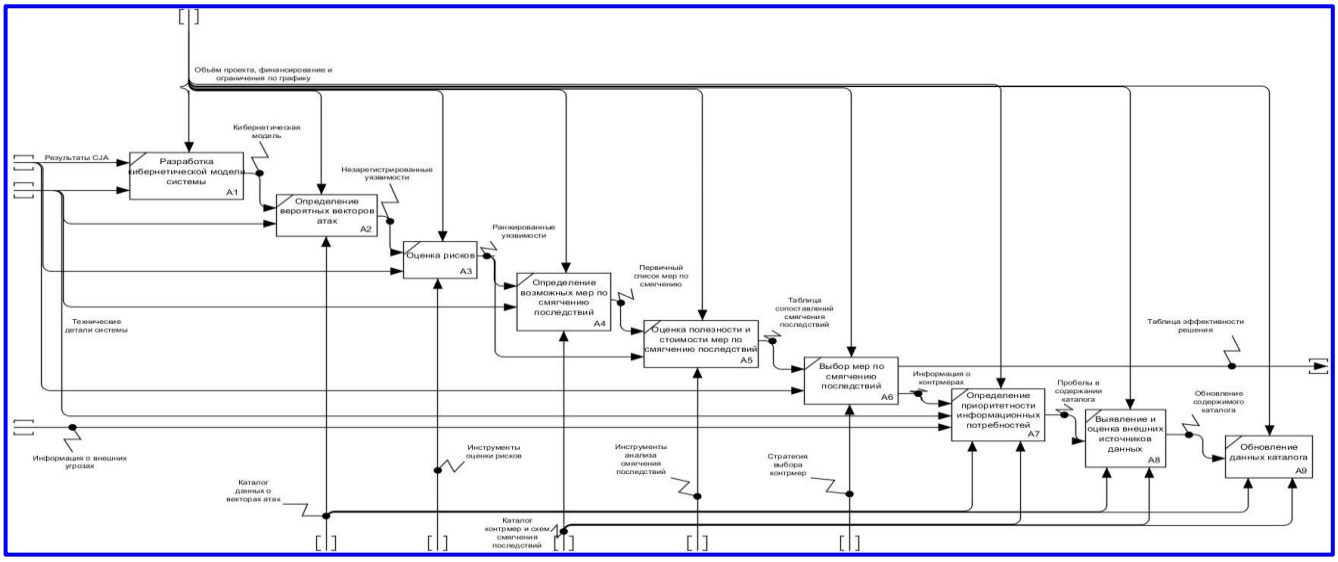

Рис. 2. Функциональная модель методологии TARA

Метод TARA включает в себя не только технические решения, но и меры по улучшению процессов управления рисками.

Правильно сформированная рекомендация включает три фрагмента информации:

1. Рекомендуемое действие, устройство, процедура или метод, то есть какую контрмеру следует применять.

2. Причина, по которой требуется выбрать данную контрмеру.

3. Последствия или эффект, если контрмера не применяется.

Одним из ключевых недостатков метода является субъективность оценки из-за различий мнений экспертов, влияющих на объективность результатов.

Заключение

События последних лет заставляют признать, что создание и обеспечение ИБ – это первостепенная задача, реализация которой необходима для поддержания жизнеспособности любой организации и предприятия.

Предприятия и организации ракетно-космической отрасли располагают множеством объектов критической инфраструктуры, которым требуется защита их цифровых данных.

Исследования в области повышения уровня ИБ указывают на то, что в последнее время использование модели PDCA становится менее релевантным. Такие методы, как DMAIC, IDEAL, ТРИЗ, TBBDI, EBBDI, могут быть более эффективными инструментами для достижения гибкости и адаптивности ИБ.

Несмотря на многообразие методов, PDCA по-прежнему остается важным инструментом управления в области ИБ, а практика показывает, что именно с привлечением метода TARA эффективность его использования может оцениваться как достаточная для достижения организацией конкурентных преимуществ в области защиты данных.

При создании СМИБ применение метода TARA в сочетании с PDCA-моделью позволяет провести более тщательный анализ угроз и рисков, а также эффективно ими управлять, выбрать оптимальные контрмеры для устранения уязвимостей и противодействия разрушению данных, а также оценить эффективность применения этих контрмер.

Способ защиты, описанный в статье, соответствует процессам обеспечения ИБ информационных активов АО «Корпорация «ВНИИЭМ» путем инвентаризации этих активов и регулярного проведения тщательной оценки рисков ИБ

Литература

1. ГОСТ Р ИСО/МЭК 27000-2021. Информационные технологии. Методы и средства обеспечения безопасности : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 мая 2021 г. № 392-ст : дата введения 2021-11-30 / подготовлен ФИЦ ИУ РАН, ООО «ИАВЦ» и АО «Эксперт». – Москва : Стандартинформ, 2021. – 24 с.

2. ГОСТ Р 58833-2020. Защита информации. Идентификация и аутентификация. Общие положения : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 10 апреля 2020 г. № 159-ст : введен впервые : дата введения 2020-05-01 / разработан ФСТЭК России, ЗАО «Аладдин Р.Д.» и ООО «НПФ «КРИСТАЛЛ». – Москва : Стандартинформ, 2020. – 28 с.

3. АО «Корпорация «ВНИИЭМ»: [Электронный ресурс]. – URL: https://www.vniiem.ru/ru.

4. ГОСТ Р ИСО 9001-2015. Системы менеджмента качества. Требования : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 сентября 2015 г. № 1391-ст : введен впервые : дата введения 2015-11-01 / подготовлен ОАО «ВНИИС». – Москва : Стандартинформ, 2015. – 24 с.

5. Threat Assessment & Remediation Analysis (TARA). Methodology Description / J. Wynn, J. Whitmore, G. Upton [et al.] // Bedford : The MITRE Corporation, 2011. – 52 p.

Поступила в редакцию 19.12.2023

***Виталий Александрович Журавлев**, бакалавр 4 курса,*
т. +7 (916) 203-39-99, e-mail: vitaalexj@mail.ru.
(РТУ МИРЭА – Российский технологический университет).
***Ксения Андреевна Соседко**, методист аспирантуры, ассистент кафедры,*
т. +7 (915) 021-27-84, e-mail: asp_ksenya_sosedko@mcc.vniiem.ru.
(АО «Корпорация «ВНИИЭМ»; РТУ МИРЭА – Российский технологический университет).

METHOD OF PROTECTING DATA FROM THE INFLUENCE OF FACTORS THAT DETERMINE THE THREATS OF ITS DESTRUCTION

V. A. Zhuravlev, K. A. Sosedko

The article deals with mechanisms for ensuring information security of ergatic systems. Improving digital technologies involves the development of information processing tools both in the implementation of creative processes and in the possibility of constructing means of destruction. The purpose of the article is to analyze the mechanisms for protecting digital information based on the objective identification of threats and the selection of countermeasures that are effective in mitigating the destructive effects of external factors (TARA). Based on the joint application of the TARA method and the PDCA model, mechanisms for creating an information security management system that increase the efficiency of ensuring the protection of transmitted messages are considered. It is shown that the use of the TARA method in combination with the PDCA model is a promising approach to ensuring information security and protecting information assets.
Key words: *information security, data protection, threat identification, selection of countermeasures, PDCA model, method TARA.*

References

1. GOST R ISO/IEC 27000-2021. Information Technology. Methods and means of ensuring safety: approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated May 19, 2021 No. 392-st : implementation date 2021-11-30 / prepared by FRC IU RAS, LLC «IAVC» and JSC «Expert». – Moscow : Standardinform, 2021. – 24 p.
2. GOST R 58833-2020. Data protection. Identification and authentication. General provisions: approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated April 10, 2020 No. 159-st : introduced for the first time: introduction date 2020-05-01 / developed by FSTEC of Russia, CJSC «Aladdin R.D.» and NPF CRYSTAL LLC. – Moscow : Standardin-form, 2020. – 28 p.
3. JSC «Corporation «VNIIEM»: [Electronic resource]. – URL: https://www.vniiem.ru/ru.
4. GOST R ISO 9001-2015. Quality management systems. Requirements: approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated September 28, 2015 № 1391-st: introduced for the first time: date of introduction 2015-11-01 / prepared by JSC VNIIS. – Moscow : Standartinform, 2015. – 24 p.
5. Threat Assessment & Remediation Analysis (TARA). Methodology Description / J. Wynn, J. Whitmore, G. Upton [et al.] // Bedford: The MITER Corporation, 2011. – 52 p.

Vitaly Alexandrovich Zhuravlev*, 4th year bachelor,*
t. +7 (916) 203-39-99, e-mail: vitaalexj@mail.ru.
(MIREA – Russian Technological University).
Ksenia Andreevna Sosedko*, Supervisor of Graduate Studies, Assistant Professor,*
t. +7 (915) 021-27-84, e-mail: asp_ksenya_sosedko@mcc.vniiem.ru.
(JSC «VNIIEM Corporation»; MIREA – Russian Technological University).