УДК 004.056.5 Вестник УрФО № 1(51) / 2024, с. 30–38

Абрамова Т.В.

DOI: 10.14529/secur240104

МНОГОАСПЕКТНЫЙ АНАЛИЗ ЧАСТНЫХ РЕШЕНИЙ В ЗАДАЧЕ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ МОНИТОРИНГА СЕТЕВОГО ТРАФИКА

В статье рассмотрены вопросы анализа эффективности частных технических решений при разработке систем защиты информации (СЗИ). Предложена многоаспектная интерактивная матричная модель (МИМ) для системного анализа характеристик технических решений, вариант применения МИМ для анализа методов и средств защиты информации на основе мониторинга сетевого трафика. Проведен многоаспектный анализ частных решений на примере методов и средств защиты информации в компьютерных сетях (КС) автоматизированных систем управления технологическим процессом (АСУ ТП) транспортировки нефтегазового сырья. Представленные в работе результаты способствуют повышению качества процесса разработки СЗИ.

Ключевые слова: *методы и средства защиты информации, многоаспектный анализ, интерактивная матричная модель, автоматизированные системы управления, мониторинг сетевого трафика.*

MULTI-ASPECT ANALYSIS OF PARTICULAR SOLUTIONS IN THE PROBLEM OF INFORMATION SECURITY BASED ON NETWORK TRAFFIC MONITORING

The article discusses the issues of analyzing the effectiveness of private technical solutions in the development of information security systems. A multi-aspect interactive matrix model (IMM) is proposed for system analysis of the characteristics of technical solutions, and an option for using IMM to analyze methods and means of information security based on network traffic monitoring. A multi-aspect analysis of particular solutions was carried out using the example of methods and means of protecting information in computer networks of automated control systems for the technological process of transporting oil and gas raw materials. The results presented in the work contribute to improving the quality of the information security development process.

Keywords: *methods and means of information security, multi-aspect analysis, interactive matrix model, automated control systems, network traffic monitoring.*

Введение

Одним из факторов успешного создания систем защиты информации (СЗИ) является наличие и рациональное использование инструментальной базы средств поиска технических решений (ТР) и оценки их эффективности на всех стадиях и этапах построения СЗИ. Большая организационная и техническая сложность проектных работ обусловила использование наряду с традиционными новых решений для повышения качества проекта, а вместе с этим – и необходимость оценки эффективности этих решений.

В научной литературе известен представительный ряд публикаций, посвященных тематике настоящей работы. В частности, в статьях [1, 2] рассматриваются вопросы оценки эффективности проектов и внедряемых систем, в [3] представлены результаты исследований вкладов отдельных технических решений в общую эффективность проекта, в [4, 5] приводятся результаты разработки систем автоматизации проектных работ по созданию СЗИ. Однако представленные в публикациях решения не позволяют в полной мере оценить эффективность конкретных методов и средств в совокупности других результатов разработок сложных проектов. Подобные задачи нередко возникают в процессе выявления актуальных стратегий при управлении проектами, а также в процессе обсуждения и принятия решений о соответствии результатов научных исследований системе требований к научно-квалификационным работам.

Целью настоящей работы является повышение качества процесса разработки СЗИ на основе системного анализа эффективности частных технических решений с использованием многоаспектной матричной модели. Для достижения цели разработана структура многоаспектной интерактивной матричной модели для системного анализа характеристик технических решений по созданию СЗИ, представлен вариант применения МИМ для анализа эффективности разработанных методов и средств в задаче построения СЗИ на ос-

нове мониторинга сетевого трафика, проведен многоаспектный анализ частных решений на примере методов и средств защиты информации в КС АСУ транспортировкой нефтегазового сырья.

Объектом исследования в настоящей работе являются СЗИ в промышленных сетях на примере КС АСУ транспортировкой нефтегазового сырья. Предметом исследования – множество методов М и множество средств С, являющихся техническими решениями для построения и совершенствования СЗИ на основе мониторинга сетевого трафика.

Структура многоаспектной интерактивной матричной модели для системного анализа характеристик технических решений по созданию СЗИ

Ниже представлена структура многоаспектной интерактивной матричной модели, демонстрирующая особенности декомпозиции процесса создания СЗИ по стадиям, структуре СЗИ и ее компонентам.

Множество аспектов А, позволяющих определить систему оценок качества технических решений, содержит следующие элементы.

1. Структурный аспект S, определяющий уровень детализации СЗИ: система, подсистема, функциональный блок. Выбор перечня функциональных блоков обусловлен особенностями решения задачи, требованиями нормативных документов к СЗИ для рассматриваемого класса систем, а так же необходимостью расширения функциональной полноты существующих средств защиты в соответствии с требованиями проекта.

2. Технологический аспект Т, определяющий стадии создания СЗИ или ее компонентов.

3. Аспект К, определяющий качество ТР на основе показателей технического, экономического, социального или иного эффекта.

Таким образом, каждое техническое решение может быть описано фасетным кодом Ф (1):

$$Ф = \{S; T; K\} \quad (1)$$

В зависимости от задачи анализа результатов исследований и разработки перечень составляющих фасетного кода дополняется такими компонентами, как: уровень актуальности R, достоверности D, практической значимости Z или другими атрибутами результатов.

Для систематизации разработанных методов и средств в модели использован способ классификации и кодирования по методике, представленной в работе [6]. Согласно предложенному способу, разработанному решению присваивается код, каждый блок которого характеризует определенный аспект анализа ТР и содержит коды подсистем СЗИ, стадий проектирования и видов эффекта, относящихся к анализируемому методу или средству.

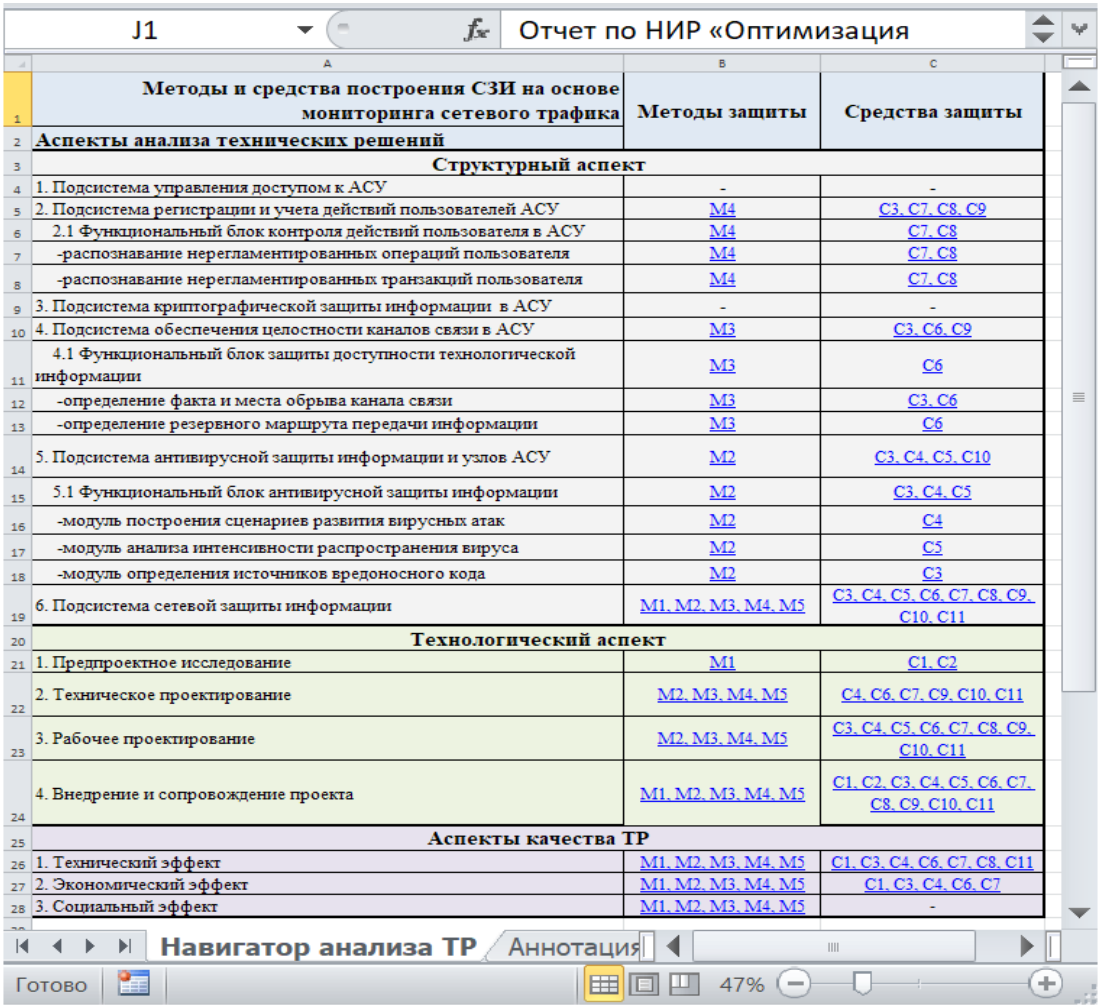
Вариант применения МИМ для анализа методов и средств защиты информации на основе мониторинга сетевого трафика

На рис. 1–3 приводится вариант реализации МИМ на основе табличного процессора MS Excel для многоаспектного анализа технических решений [7, 8], полученных по итогам научных исследований по теме гранта РФФИ № 18-47-560012 «Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков» [9]. МИМ включает навигатор анализа ТР, аннотации технических решений и характеристику решений по каждому из аспектов, представленных в выражении (1).

На рис. 1 представлена экранная форма навигатора анализа технических решений, отображающего общую структуру МИМ и позволяющего определить место разработанных решений в структуре СЗИ, этапы проектирования, на которых они применяются, и вид получаемого эффекта. Ввод сведений о технических решениях осуществляется с использованием специальных опросных анкет, реализованных в табличном процессоре MS Excel.

На рис. 2 представлен фрагмент аннотации ТР, содержащей код и наименование решения, общие сведения о ТР и ссылки на соответствующие электронные ресурсы в сети Internet.

Переход к сведениям о ТР и результатам анализа их эффективности осуществляется со страницы навигатора по гиперссылкам, обеспечивающим интерактивность модели и быструю навигацию между сведениями о решении, результатами анализа по различным аспектам и соответствующими электронными ресурсами сети Internet. Например, при нажатии на ссылку М2 в поле навигатора (рис. 1), характеризующего определенный аспект анализа, выводится информация об эффективности метода М2 «Метод восстановления

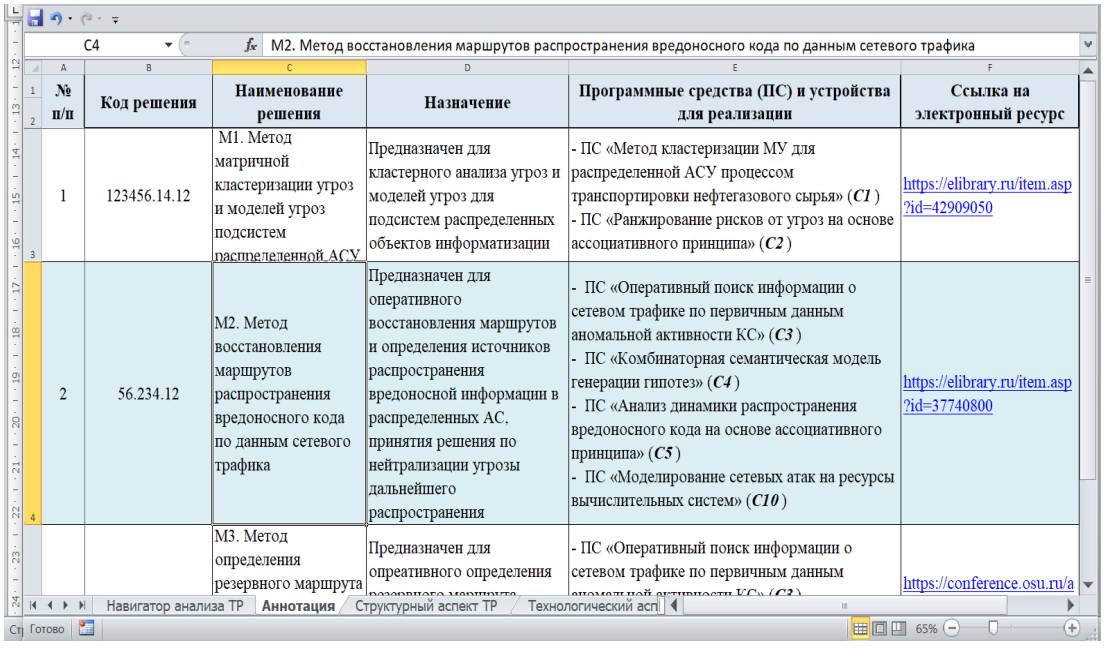


J1 | Отчет по НИР «Оптимизация

Методы и средства построения СЗИ на основе мониторинга сетевого трафика	Методы защиты	Средства защиты
Аспекты анализа технических решений		
Структурный аспект		
1. Подсистема управления доступом к АСУ	-	-
2. Подсистема регистрации и учета действий пользователей АСУ	M4	C3, C7, C8, C9
2.1 Функциональный блок контроля действий пользователя в АСУ	M4	C7, C8
-распознавание нерегламентированных операций пользователя	M4	C7, C8
-распознавание нерегламентированных транзакций пользователя	M4	C7, C8
3. Подсистема криптографической защиты информации в АСУ	-	-
4. Подсистема обеспечения целостности каналов связи в АСУ	M3	C3, C6, C9
4.1 Функциональный блок защиты доступности технологической информации	M3	C6
-определение факта и места обрыва канала связи	M3	C3, C6
-определение резервного маршрута передачи информации	M3	C6
5. Подсистема антивирусной защиты информации и узлов АСУ	M2	C3, C4, C5, C10
5.1 Функциональный блок антивирусной защиты информации	M2	C3, C4, C5
-модуль построения сценариев развития вирусных атак	M2	C4
-модуль анализа интенсивности распространения вируса	M2	C5
-модуль определения источников вредоносного кода	M2	C3
6. Подсистема сетевой защиты информации	M1, M2, M3, M4, M5	C3, C4, C5, C6, C7, C8, C9, C10, C11
Технологический аспект		
1. Предпроектное исследование	M1	C1, C2
2. Техническое проектирование	M2, M3, M4, M5	C4, C6, C7, C9, C10, C11
3. Рабочее проектирование	M2, M3, M4, M5	C3, C4, C5, C6, C7, C8, C9, C10, C11
4. Внедрение и сопровождение проекта	M1, M2, M3, M4, M5	C1, C2, C3, C4, C5, C6, C7, C8, C9, C10, C11
Аспекты качества ТР		
1. Технический эффект	M1, M2, M3, M4, M5	C1, C3, C4, C6, C7, C8, C11
2. Экономический эффект	M1, M2, M3, M4, M5	C1, C3, C4, C6, C7
3. Социальный эффект	M1, M2, M3, M4, M5	-

Навигатор анализа ТР | Аннотация | Готово | 47%

Рис. 1. Экранная форма навигатора анализа технических решений



C4 | M2. Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика

№ п/п	Код решения	Наименование решения	Назначение	Программные средства (ПС) и устройства для реализации	Ссылка на электронный ресурс
1	123456.14.12	M1. Метод матричной кластеризации угроз и моделей угроз подсистем распределенной АСУ	Предназначен для кластерного анализа угроз и моделей угроз для подсистем распределенных объектов информатизации	- ПС «Метод кластеризации МУ для распределенной АСУ процессом транспортировки нефтегазового сырья» (***C1***) - ПС «Ранжирование рисков от угроз на основе ассоциативного принципа» (***C2***)	https://elibrary.ru/item.asp?id=42909050
2	56.234.12	M2. Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	Предназначен для оперативного восстановления маршрутов и определения источников распространения вредоносной информации в распределенных АС, принятия решения по нейтрализации угрозы дальнейшего распространения	- ПС «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности КС» (***C3***) - ПС «Комбинаторная семантическая модель генерации гипотез» (***C4***) - ПС «Анализ динамики распространения вредоносного кода на основе ассоциативного принципа» (***C5***) - ПС «Моделирование сетевых атак на ресурсы вычислительных систем» (***C10***)	https://elibrary.ru/item.asp?id=37740800
		M3. Метод определения резервного маршрута	Предназначен для опреативного определения	- ПС «Оперативный поиск информации о сетевом трафике по первичным данным	https://conference.osu.ru/a

Навигатор анализа ТР | Аннотация | Структурный аспект ТР | Технологический асп | Готово | 65%

Рис. 2. Экранная форма аннотации технических решений

маршрутов распространения вредоносного кода по данным сетевого трафика» по соответствующему аспекту. Строка сведений об анализируемом методе выделяется цветом.

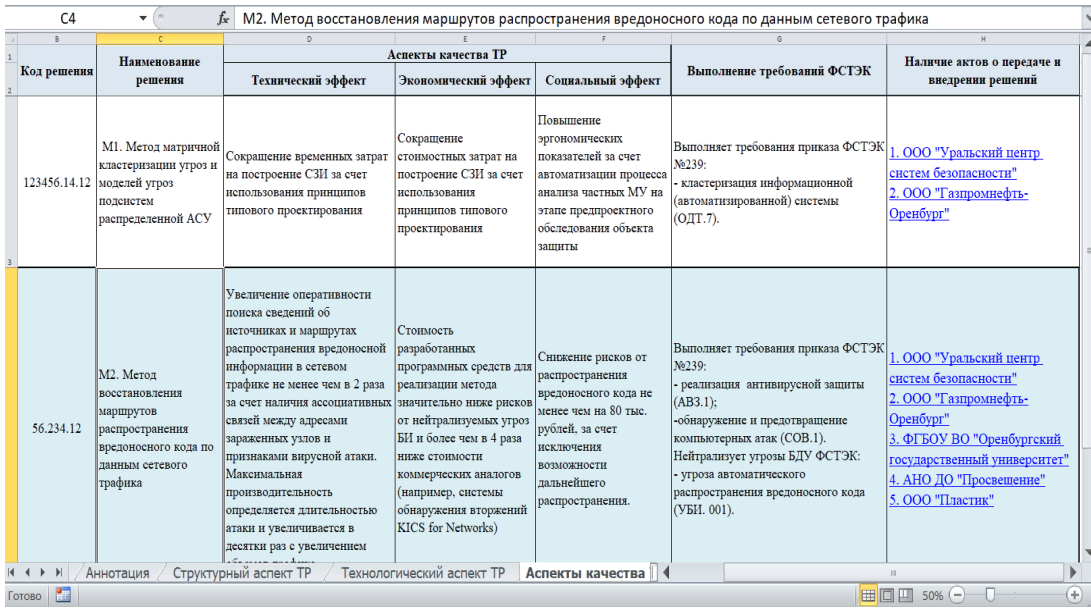
Многоаспектный анализ частных решений на примере методов и средств защиты информации в КС АСУ транспортировкой нефтегазового сырья

Анализ решений по *структурному аспекту* осуществляется согласно требованиям стандарта [10]. Относительно представленного в примере метода М2 можно сделать вывод, что метод используется в подсистемах антивирусной и сетевой защиты информации и позволяет повысить функциональную полноту средств антивирусной защиты за счет функций построения маршрутов и определения источников распространения вредоносного кода в КС.

Анализ решений по *технологическому аспекту* осуществляется согласно положениям стандарта [11]. В результате анализа делается вывод о том, на каком этапе проекта используется разработанное решение. Например, модели, разработанные при реализации метода М2, используются на этапе технического проектирования, а программное обеспечение – на этапах рабочего проектирования, внедрения и сопровождения проекта.

Анализ решений по *аспектам качества ТР* проводится с учетом технического, экономического и социального эффекта от его использования. Численные значения показателей эффекта выводятся на основе данных опросных анкет, заполняемых авторами разработанных решений. Результаты анализа позволяют оценить эффективность от внедрения ТР, степень выполнения требований нормативных документов Федеральной службы по техническому и экспортному контролю (ФСТЭК России), наиболее значимых при построении СЗИ для исследуемого объекта, нейтрализуемые угрозы из банка данных угроз ФСТЭК [12] и степень снижения рисков от угроз.

На рис. 3 в качестве примера представлена экранная форма результатов анализа эффективности метода М2 по аспектам качества ТР.


C4 | M2. Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика

Код решения	Наименование решения	Аспекты качества ТР: Технический эффект	Аспекты качества ТР: Экономический эффект	Аспекты качества ТР: Социальный эффект	Выполнение требований ФСТЭК	Наличие актов о передаче и внедрении решений
123456.14.12	М1. Метод матричной кластеризации угроз и моделей угроз подсистем распределенной АСУ	Сокращение временных затрат на построение СЗИ за счет использования принципов типового проектирования	Сокращение стоимостных затрат на построение СЗИ за счет использования принципов типового проектирования	Повышение эргономических показателей за счет автоматизации процесса анализа частных МУ на этапе предпроектного обследования объекта защиты	Выполняет требования приказа ФСТЭК №239: - кластеризация информационной (автоматизированной) системы (ОДТ.7).	1. ООО "Уральский центр систем безопасности" 2. ООО "Газпромнефть-Оренбург"
56.234.12	М2. Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	Увеличение оперативности поиска сведений об источниках и маршрутах распространения вредоносной информации в сетевом трафике не менее чем в 2 раза за счет наличия ассоциативных связей между адресами зараженных узлов и признаками вирусной атаки. Максимальная производительность определяется длительностью атаки и увеличивается в десятки раз с увеличением	Стоимость разработанных программных средств для реализации метода значительно ниже рисков от нейтрализуемых угроз БИ и более чем в 4 раза ниже стоимости коммерческих аналогов (например, системы обнаружения вторжений KICS for Networks)	Снижение рисков от распространения вредоносного кода не менее чем на 80 тыс. рублей, за счет исключения возможности дальнейшего распространения.	Выполняет требования приказа ФСТЭК №239: - реализация антивирусной защиты (АВЗ.1); -обнаружение и предотвращение компьютерных атак (СОВ.1). Нейтрализует угрозы БДУ ФСТЭК: - угроза автоматического распространения вредоносного кода (УБИ. 001).	1. ООО "Уральский центр систем безопасности" 2. ООО "Газпромнефть-Оренбург" 3. ФГБОУ ВО "Оренбургский государственный университет" 4. АНО ДО "Просвещение" 5. ООО "Пластик"

Аннотация | Структурный аспект ТР | Технологический аспект ТР | Аспекты качества

Готово 50%

Рис. 3. Экранная форма результатов анализа эффективности метода по аспектам качества ТР

Сведения о наличии актов о передаче и внедрении технических решений на отраслевых предприятиях необходимы для подтверждения новизны и достоверности анализируемых методов и средств.

Результаты многоаспектного анализа частных решений на примере методов и средств защиты информации в КС АСУ транспортировкой нефтегазового сырья, полученных при выполнении проекта [9], представлены в табл. 1.

Предложенная модель отличается применением принципов многоаспектности и интерактивности, что позволяет оперативно проводить системный анализ эффективности частных технических решений на всех стадиях разработки СЗИ и способствует повышению качества процесса разработки.

Таблица 1

Результаты многоаспектного анализа эффективности методов и средств защиты информации в КС АСУ транспортировкой нефтегазового сырья

Метод	Результаты анализа	Средства для реализации метода
Метод матричной кластеризации угроз и моделей угроз (МУ) подсистем распределенной АСУ (М1)	– предназначен для кластерного анализа моделей угроз (МУ) для подсистем распределенных объектов информатизации на этапах предпроектного исследования, внедрения и сопровождения проекта; – используется во всех подсистемах СЗИ; – позволяет повысить функциональную полноту методов и средств кластеризации элементов АС, согласно мерам ОДТ. 7 приказа ФСТЭК №239; – позволяет снизить временные и стоимостные затраты на построение СЗИ.	– ПС «Метод кластеризации МУ для распределенной АСУ процессом транспортировки нефтегазового сырья» (С1); – ПС «Ранжирование рисков от угроз на основе ассоциативного принципа» (С2).
Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика (М2)	– предназначен для оперативного восстановления маршрутов и определения источников распространения вредоносной информации в распределенных АС и принятия решения по нейтрализации угрозы дальнейшего распространения; – используется на этапах технического и рабочего проектирования, внедрения и сопровождения подсистем антивирусной и сетевой защиты информации; – позволяет повысить функциональную полноту методов и средств антивирусной защиты, согласно мерам АВ3.1 и СОВ.1 приказа ФСТЭК №239; – позволяет повысить оперативность поиска данных о распространении вредоносной информации в сетевом трафике не менее чем в 2 раза за счет принципов ассоциативности и снизить риски от угрозы распространения вредоносного кода в КС не менее чем на 80 тыс. рублей	– ПС «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности КС» (С3); – ПС «Комбинаторная семантическая модель генерации гипотез» (С4); – ПС «Анализ динамики распространения вредоносного кода на основе ассоциативного принципа» (С5); – ПС «Моделирование сетевых атак на ресурсы вычислительных систем» (С10).
Метод определения резервного маршрута на основе принципов обхода аномальных участков промышленных КС (М3)	– предназначен для определения резервного маршрута передачи информации при блокировании одного или нескольких участков основного канала связи; – используется на этапах технического и рабочего проектирования, внедрения и сопровождения подсистем обеспечения целостности и доступности технологической информации и сетевой защиты информации; – позволяет повысить функциональную полноту средств защиты доступности информации в АС, согласно мерам ЗИС. 6 и ДНС.4 приказа ФСТЭК №239; – позволяет снизить риски потери информации о состоянии объекта защиты не менее чем на 14% за счет использования принципов горячего резервирования и оперативного определения резервного маршрута передачи данных.	– ПС «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности КС» (С3); – ПС «Маршрутизация сетевых потоков в режимах переключения на резервные каналы связи» (С6).

Продолжение табл. 1

Метод мониторинга действий персонала в АС на основе логического контроля ассоциативности сигнатур управляющих транзакций (М4)	– предназначен для контроля управляющих операций и транзакций в АС; – используется на этапах технического и рабочего проектирования, внедрения и сопровождения подсистем регистрации и учета, сетевой защиты информации; – позволяет повысить функциональную полноту методов и средств контроля действий пользователей в АС, согласно мерам АУД. 9 и ОЦЛ. 5 приказа ФСТЭК №239; – метод позволяет снизить риски от угрозы несанкционированных действий персонала АСУ не менее чем в 2 раза за счет контроля последовательности и очередности подачи управляющих команд	– ПС «Метод мониторинга управляющих команд оператора АСУ на основе данных протокола Modbus TCP» (С7); – ПС «Моделирование сетевого трафика на базе протокола TCP/ModBUS» (С9); – устройство для контроля поведения пользователя (С8).
Метод обнаружения аномалий в сетевом трафике на основе дихотомического подхода (М5)	– предназначен для обнаружения аномалий в сетевом трафике КС; – используется на этапах технического и рабочего проектирования, внедрения и сопровождения подсистемы сетевой защиты информации; – позволяет повысить функциональную полноту методов и средств анализа сетевого трафика, согласно мерам АУД. 5 и СОВ.1 приказа ФСТЭК №239; – метод обладает большей оперативностью и меньшей вычислительной сложностью на этапе распознавания аномалии не менее чем на порядок по сравнению с базовыми, в частности, нейросетевыми методами.	– ПС «Метод дихотомического распознавания аномалий в сетевом трафике» (С11).

Заключение

Разработанная интерактивная матричная модель позволяет:

– автоматизировать процедуру обоснования и доказательства применимости результатов научных исследований;

– выявить избыточность или дефицит методов и средств защиты информации для конкретного этапа проекта;

– оценить эффективность результатов конкретных решений в совокупности других результатов разработок сложных проектов;

– оценить вклад разработанных методов и средств в общий результат проекта.

Представленные результаты могут быть использованы при составлении отчетов по научно-исследовательской работе с учетом актуальности и значимости конкретных технических решений.

Литература

1. Вишнякова Т.О., Васильев В.И. Анализ эффективности систем физической защиты при помощи марковской сетевой модели // Вестник УГАТУ = Vestnik UGATU. 2007. №7. URL: https://cyberleninka.ru/article/n/analiz-effektivnosti-sistem-fizicheskoy-zaschity-pri-pomoschi-markovskoy-setevoy-modeli (дата обращения: 23.12.2023).

2. Хубаев Г.Н. Сравнение сложных программных систем по критерию функциональной полноты // Программные продукты и системы (SOFTWARE&SYSTEMS). – 1998. – №2. – С.6-9.

3. Коломойцев В.С. Модели и методы оценки эффективности систем защиты информации и обоснование выбора их комплектации: автореферат дис. ... кандидата технических наук: 05.13.19 / Коломойцев Владимир Сергеевич; [Место защиты: С.-Петерб. гос. ун-т телекоммуникаций им. М.А. Бонч-Бруевича]. - Санкт-Петербург, 2018. - 20 с.

4. Домарев В.В. Моделирование процессов создания и оценки эффективности систем защиты информации [Электронный ресурс]. - URL: http://citforum.ru/security/articles/model_proc. (дата обращения 23.12.2023).

5. Касимов А.Ф. Автоматизация проектирования систем защиты информации с использованием

методов многоальтернативной оптимизации : автореферат дис. ... кандидата технических наук: 05.13.12 / Воронеж. гос. техн. ун-т. - Воронеж, 2005. - 17 с.

6. Смирнова, Г.Н. Проектирование экономических информационных систем [Текст]: учебное пособие / Г.Н. Смирнова, Ю. Ф. Тельнов; Международный консорциум «Электронный ун-т», Московский гос. ун-т экономики, статистики и информатики, Евразийский открытый ин-т. - Москва: МЭСИ, 2004. - 22 см.; ISBN 5-7764-0405-3.

7. Патент 2675896 Российская Федерация, МПК G06K9/62. Устройство для контроля поведения пользователя/Абрамова Т.В., Аралбаев Т.З., Каскинов И.И., Хатеев М.Д./заявитель и патентообладатель ОГУ. – № 2018100997/08; заявл. 10.01.2018; опубл. 25.12.2018, Бюл. № 36. – 17 с.

8. Университетский фонд электронных ресурсов. Оренбургский государственный университет. - URL: https://ufer.osu.ru/ (дата обращения 23.12.2023).

9. Аралбаев, Т.З. Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков: монография/Т.З. Аралбаев, Г.Г. Аралбаева, Т.В. Абрамова, Р.Р. Галимов, А.В. Манжосов. - Оренбург: ОГУ, 2018.

10. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. [Электронный ресурс]. – URL: https://itsec2012.ru/gosudarstvennyy-standart-rossiyskoy-federacii-gost-r-51624-2000-zashchita-informacii (дата обращения 23.12.2023).

11. ГОСТ Р 59793-2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания [Электронный ресурс]. – URL: https://www.astoni.ru/upload/iblock/2d4/GOST-34.601_90.pdf (дата обращения 23.12.2023).

12. Банк данных угроз безопасности информации. Федеральная служба по техническому и экспортному контролю ФСТЭК России, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – URL: https://bdu.fstec.ru/ (дата обращения 31.01.2024).

References

1. Vishnyakova T.O., Vasil'ev V.I. Analiz effektivnosti sistem fizicheskoy zashchity pri pomoshchi markovskoy setevoy modeli // Vestnik UGATU = Vestnik UGATU. 2007. №7. URL: https://cyberleninka.ru/article/n/analiz-effektivnosti-sistem-fizicheskoy-zaschity-pri-pomoschi-markovskoy-setevoy-modeli (data obrashcheniya: 23.12.2023).

2. Khubaev G.N. Sravnenie slozhnykh programmnykh sistem po kriteriyu funktsional'noy polnoty // Programmnye produkty i sistemy (SOFTWARE&SYSTEMS). – 1998. – №2. – S.6-9.

3. Kolomoytsev V.S. Modeli i metody otsenki effektivnosti sistem za-shchity informatsii i obosnovanie vybora ikh komplektatsii: avtoreferat dissertatsii na soiskanie uchenoy stepeni kandidata tekhnicheskikh nauk: 05.13.19 / Kolomoytsev Vladimir Sergeevich; [Mesto zashchity: Sankt-Peterburgskiy. gos. un-t telekommunikatsiy im. M.A. Bonch-Bruevicha]. - Sankt-Peterburg, 2018. - 20 s.

4. Domarev V.V. Modelirovanie protsessov sozdaniya i otsenki effektivnosti sistem zashchity informatsii [Elektronnyy resurs]. - URL: http://citforum.ru/security/articles/model_proc. (data obrashcheniya 23.12.2023).

5. Kasimov A.F. Avtomatizatsiya proektirovaniya sistem zashchity informatsii s ispol'zovaniem metodov mnogoal'ternativnoy optimizatsii: avtoreferat dissertatsii na soiskanie uchenoy stepeni kandidata tekhnicheskikh nauk: 05.13.12 / Voronezh. gos. tekhnicheskiy un-t. - Voronezh, 2005. - 17 s.

6. Smirnova, G.N. Proektirovanie ekonomicheskikh informatsionnykh sistem [Tekst]: uchebnoe posobie / G. N. Smirnova, Yu. F. Tel'nov; Mezhdunarodnyy konsortsium "Elektronnyy un-t", Moskovskiy gos. un-t ekonomiki, statistiki i informatiki, Evraziyskiy otkrytyy in-t. - Moskva: MESI, 2004. - 22 sm.; ISBN 5-7764-0405-3.

7. Patent 2675896 Rossiyskaya Federatsiya, MPK G06K9/62. Ustroystvo dlya kontrolya povedeniya pol'zovatelya/Abramova T.V., Aralbaev T.Z., Kaskinov I.I., Khateev M.D./zayavitel' i patentoobladatel' OGU. – № 2018100997/08; zayavl. 10.01.2018; opubl. 25.12.2018, Byul. № 36. – 17 s.

8. Universitetskiy fond elektronnykh resursov. Orenburgskiy gosudarstvennyy universitet. - URL: https://ufer.osu.ru/ (data obrashcheniya 23.12.2023).

9. Aralbaev, T.Z. Optimizatsiya metodov kontrolya tekhnicheskogo sostoyaniya raspredelennykh avtomatizirovannykh sistem v usloviyakh vozdeystviya prostranstvenno-vremennykh ugroz na osnove monitoringa setevykh informatsionnykh potokov: monografiya/T.Z. Aralbaev, G.G. Aralbaeva, T.V. Abramova, R.R. Galimov, A.V. Manzhosov. - Orenburg: OGU, 2018.

10. GOST R 51624-2000. Zashchita informatsii. Avtomatizirovannye siste-my v zashchishchennom ispolnenii. Obshchie trebovaniya. [Elektronnyy resurs]. – URL: https://itsec2012.ru/gosudarstvennyy-standart-rossiyskoy-federacii-gost-r-51624-2000-zashchita-informacii (data obrashcheniya 23.12.2023).

11. GOST R 59793-2021 Informatsionnye tekhnologii. Kompleks standartov na avtomatizirovannye sistemy. Avtomatizirovannye sistemy. Stadii sozdaniya [Elektronnyy resurs]. – URL: https://www.astoni.ru/upload/iblock/2d4/GOST-34.601_90.pdf (data obrashcheniya 23.12.2023).

12. Bank dannykh ugroz bezopasnosti informatsii. Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu FSTEK Rossii, Gosudarstvennyy nauchno-issledovatel'skiy ispytatel'nyy institut problem tekhnicheskoy za-shchity informatsii FAU «GNIII PTZI FSTEK Rossii». – URL: https://bdu.fstec.ru/ (data obrashcheniya 31.01.2024).

АБРАМОВА Таисия Вячеславовна, старший преподаватель кафедры вычислительной техники и защиты информации федерального государственного бюджетного образовательного учреждения «Оренбургский государственный университет». 460018, г. Оренбург, проспект Победы, д. 13. E-mail: taya357@gmail.com

ABRAMOVA Taisiya Vyacheslavovna, senior lecturer at the Department of Computer Science and Information Security, Federal State Budgetary Educational Institution of Higher Education «Orenburg State University». 460018, Orenburg, ave. Pobeda, 13. E-mail: taya357@gmail.com