Индекс 79187

ISSN 2073-2600

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

2

(137)

Подписывайтесь,

читайте,

пишите в наш журнал

Москва 2022

Все новейшие достижения и современные разработки предприятий оборонного комплекса — в научно-технических журналах ФГУП «НТЦ оборонного комплекса «Компас»

ФГУП «Научно-технический центр оборонного комплекса «Компас» является издателем следующих научных журналов:

Межотраслевой научно-технический журнал

Оборонный комплекс — научно-техническому прогрессу России
(4 выпуска)

Подписной индекс **79379**

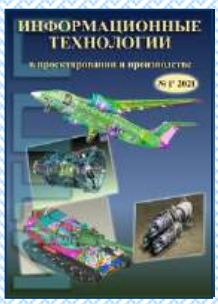
Издается с 1984 года

Межотраслевой научно-технический журнал

Конструкции из композиционных материалов
(4 выпуска)

Подписной индекс **80089**

Издается с 1981 года



Научно-технический журнал

Информационные технологии в проектировании и производстве
(4 выпуска)

Подписной индекс **79378**

Издается с 1976 года

Межотраслевой научно-практический журнал

Экология промышленного производства
(4 выпуска)

Подписной индекс **80090**

Издается с 1993 года

Научно-практический журнал

Вопросы защиты информации
(4 выпуска)

Подписной индекс **79187**

Издается с 1974 года

Все издания ФГУП "Научно-технический центр оборонного комплекса «Компас»:

✓ *включены решением ВАК Министерства науки и высшего образования России в перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата и доктора наук;*

✓ *метаданные выпусков включены в базу данных Российского индекса научного цитирования (РИНЦ).*

Более подробную информацию об изданиях, подписке, дополнительных услугах можно получить
по тел.: 8 (495) 491-43-17, 8 (495) 491-77-67, 8 (495) 491-77-20 (*подписка*);
факс: 8 (495) 491-44-80.
E-mail: izdanie@ntckompas.ru

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
«НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР ОБОРОННОГО КОМПЛЕКСА «КОМПАС»
(ФГУП «НТЦ ОБОРОННОГО КОМПЛЕКСА «КОМПАС»)

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

2 (137)

Москва 2022
Основан в 1974 г.

СОДЕРЖАНИЕ

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2022.
Вып. 2 (137). С. 1—56.

Редактор *О. А. Константинова*
Компьютерная верстка: *Н. В. Ильина*, *К. В. Трыкина*

Подписано в печать 20.06.2022. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 7,0. Уч.-изд. л. 7,2.
Тираж 400 экз. Заказ 1996. Свободная цена.
Адрес редакции: 125424, Москва,
Волоколамское ш., 77. ФГУП «НТЦ оборонного комплекса «Компас».
http://ntckompas.ru
Отпечатано: 101000, Москва,
Лубянский проезд, д. 15, стр. 4, офис 105.
ИП Кириченко Алексей Викторович.
Индекс 79187.

УДК 004.942
DOI: 10.52190/2073-2600_2022_2_3
EDN: IZNQRQ

Функциональная модель синтеза скрипта контроля системы обнаружения, предупреждения и ликвидации последствий компьютерных атак

С. А. Коноваленко, канд. техн. наук
Краснодарское высшее военное училище им. генерала армии С. М. Штеменко,
г. Краснодар, Россия

На основе методологии IDEF0 разработана функциональная модель синтеза скрипта для локального измерения значений параметрических данных, характеризующих состояние процесса функционирования системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА). В состав функциональной модели синтеза скрипта контроля СОПКА включено множество функций, определение которых осуществлено в виде стратегий, представляемых посредством треугольных таблиц, состоящих из частично упорядоченных последовательностей выделенных операций, обеспечивающих возможность повышения эффективности процесса контроля состояния СОПКА, функционирующей в различных режимах и условиях эксплуатации.

Ключевые слова: контроль, скрипт, система обнаружения, предупреждения и ликвидации последствий компьютерных атак.

В целях эффективного применения системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА) в различных режимах и условиях эксплуатации необходимо с минимальным уровнем расхода операционных ресурсов всех видов своевременно осуществлять контроль состояния ее процесса функционирования (ПФ) [1—5]. Для решения задачи контроля состояния ПФ СОПКА в [6] разработана модель системы адаптивного контроля (САК), в составе которой выделена подсистема пассивного контроля (ППК) соответствующего объекта. Указанная ППК САК обеспечивает реализацию пассивного удаленного и пассивного локального контроля состояния ПФ СОПКА с возможностью изменения последовательности их применения во времени, приближенном к реальному, с учетом функционирования объекта контроля в условиях часто появляющихся фактов неустойчивых сетевых взаимодействий (НСВ) с САК [6—9].

Коноваленко Сергей Александрович, старший преподаватель.
E-mail: konovalenko_rcf@mail.ru

Статья поступила в редакцию 23 мая 2022 г.

При учете того, что в [7—9] был разработан подход, описывающий пассивный удаленный контроль состояния ПФ соответствующего объекта, в данной работе осуществим синтез пассивного локального контроля состояния ПФ СОПКА, что в комплексе обеспечит возможность практической реализации модели САК [6].

Синтез пассивного локального контроля состояния ПФ СОПКА осуществим на основе модели САК [6] при следующих ограничениях:

1. При решении поставленной задачи учитываются процессы, реализуемые исключительно модулем локального измерения типа, состояния ПФ СОПКА и ее условий эксплуатации, а именно [6]:

- синтез скрипта для локального измерения значений параметрических данных (ПД), характеризующих состояние ПФ специализированного средства (СС) СОПКА, в условиях часто появляющихся фактов НСВ САК с объектом контроля;
- отправка скрипта в адрес СС СОПКА, функционирующего в условиях часто появляющихся фактов НСВ с САК, для локального измерения значений ПД, характеризующих состояние его ПФ;

- вычисление значения контрольного момента времени получения результатов выполнения скрипта на СС СОПКА, функционирующем в условиях часто появляющихся фактов НСВ с САК;
- ожидание поступления результатов выполнения скрипта на СС СОПКА, функционирующем в условиях часто появляющихся фактов НСВ с САК;
- запрос на получение результатов выполнения скрипта на СС СОПКА, функционирующем в условиях часто появляющихся фактов НСВ с САК;
- прием результатов выполнения скрипта на СС СОПКА, функционирующем в условиях часто появляющихся фактов НСВ с САК;
- проверка уровня полноты результатов выполнения скрипта в целях снижения уровня расхода операционных ресурсов всех видов на реализацию ПФ САК.

2. Наиболее слабоструктурированным процессом является синтез скрипта для локального измерения значений ПД, характеризующих состояние ПФ СС СОПКА $\left(\mathcal{V}_{\text{сск}}^{\text{лизм}}(t)\right)$.

С учетом указанных ограничений решение задачи синтеза пассивного локального контроля сведем к определению $\mathcal{V}_{\text{сск}}^{\text{лизм}}(t)$, для чего построим функциональную модель соответствующего процесса, представленную в виде диаграмм узлов А0 и А1 (рис. 1, 2) [1, 2, 5, 10—13].

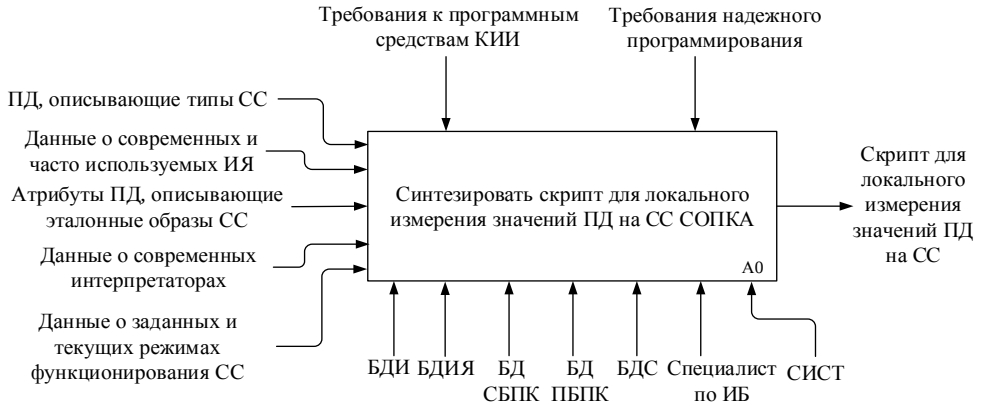


Рис. 1. Диаграмма "Синтезировать скрипт для локального измерения значений ПД на СС СОПКА", узел А0

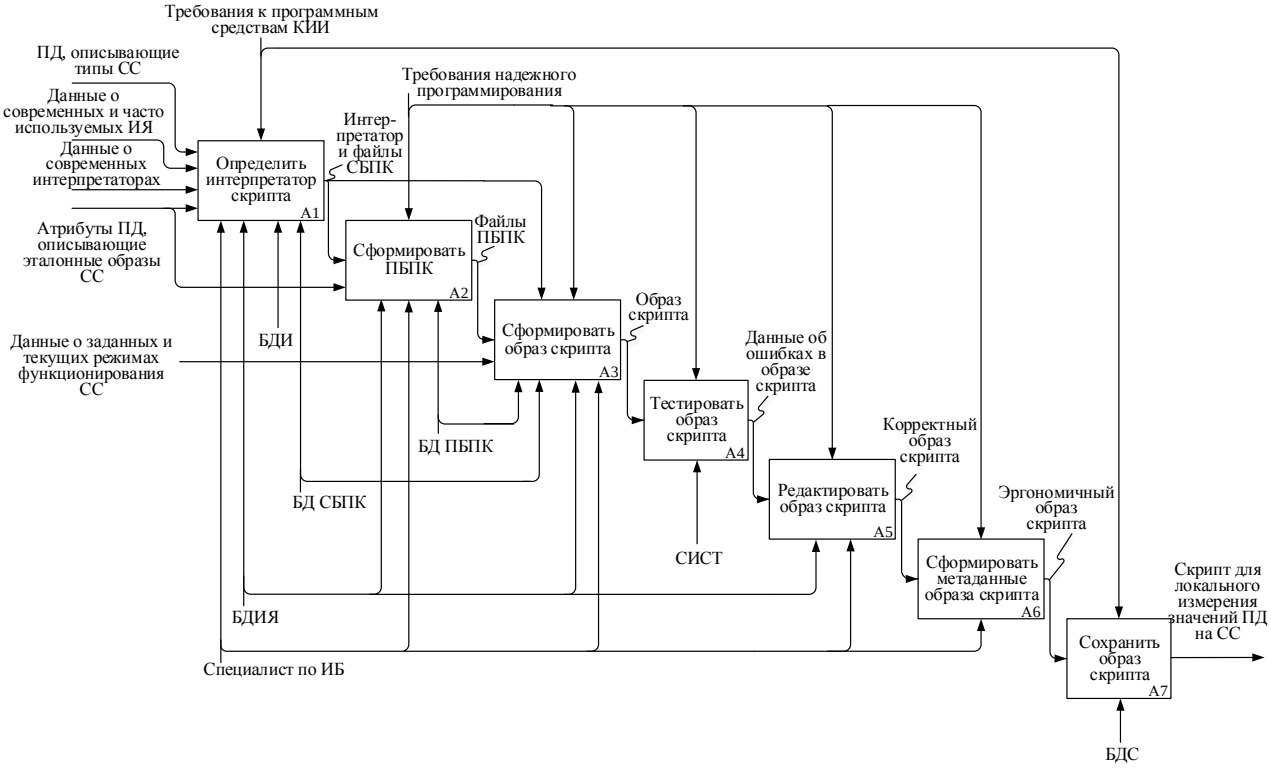


Рис. 2. Диаграмма "Синтезировать скрипт для локального измерения значений ПД на СС СОПКА", узел А1

Отметим, что в разработанной функциональной модели процесса $\mathcal{U}_{\text{сск}}^{\text{лизм}}(t)$ (рис. 1, 2) [10, 11, 13—16]:

1. База данных интерпретаторов (БДИ) предназначена для хранения множества программ, способных анализировать, обрабатывать и немедленно выполнять набор инструкций (команд), образующих скрипт для локального измерения значений ПД на СС СОПКА.

2. База данных интерпретируемых языков (БДИЯ) предназначена для хранения множества интерпретируемых языков (ИЯ), обеспечивающих возможность синтеза скрипта для локального измерения значений ПД на СС СОПКА.

3. База данных стандартных библиотек программных кодов (БД СБПК) предназначена для хранения множества файлов, содержащих описания общепринятых (часто встречающихся) функций, обеспечивающих локальное измерение значений базовых атрибутов ПД на СС СОПКА посредством соответствующих интерпретаторов, входящих в БДИ.

4. База данных пользовательских библиотек программных кодов (БД ПБПК) предназначена для хранения множества файлов, содержащих описания уникальных функций, обеспечивающих локальное измерение значений специфичных атрибутов ПД на СС СОПКА посредством соответствующих интерпретаторов, входящих в БДИ.

5. База данных скриптов (БДС) предназначена для хранения множества скриптов для локального измерения значений ПД на СС СОПКА.

6. Специализированное инструментальное средство тестирования (СИСТ) предназначено для обнаружения ошибок в образе скрипта для локального измерения значений ПД на СС СОПКА.

На основе вышеуказанного и в целях дальнейшей формализации процесса $\mathcal{U}_{\text{сск}}^{\text{лизм}}(t)$ (рис. 2) введем следующие допущения:

- функции "тестировать образ скрипта", "редактировать образ скрипта", "сформировать метаданные образа скрипта", "сохранить образ скрипта" считаем заданными [10, 11, 13, 15, 16] и далее не рассматриваем;
- под данными об ошибках в образе скрипта понимаем информацию, свидетельствующую о ситуациях, в которых порядок и результат выполнения скрипта для локального измерения значений ПД на СС СОПКА является не соответствующим заданным целям его применения [4, 16, 17];
- под корректным образом скрипта понимаем состояние, при котором в скрипте для локального измерения значений ПД на СС СОПКА отсутствуют ошибки, влияющие на достижение заданных целей его применения [4, 16, 17];
- под метаданными образа скрипта понимаем информацию, содержащую пояснения (комментарии) к набору инструкций, образующих скрипт для локального измерения значений ПД на СС СОПКА [4, 16, 17];
- под эргономичным образом скрипта понимаем состояние, при котором скрипт для локального измерения значений ПД на СС СОПКА является легким в понимании набора инструкций, образующих его, и обеспечивающим с минимальной вероятностью внесения ошибок возможность его модификации [4, 16, 17].

Исходя из введенных допущений требуется (рис. 2):

$$\mathcal{U}_{\text{сск}}^{\text{лизм}}(t)\colon s_{\hbar}^{\text{и}} \xrightarrow{\mathcal{V}_{\hbar}^{\text{ск}}} s_{\hbar}^{\text{к}} \Big| \mathcal{V}_{\hbar}^{\text{ск}} = \bigcup_{\text{ƛ}=1}^{\ell} v_{\text{ƛ}}^{\hbar} \to opt, \quad \hbar = \overline{1,3}, \tag{1}$$

где $\mathcal{V}_{\hbar}^{\text{ск}}$ — произвольная ($\hbar$) функция, реализующая процесс $\mathcal{U}_{\text{сск}}^{\text{лизм}}(t)$;

$s_{\hbar}^{\text{и}}$ — исходная ситуация (состояние) на момент начала выполнения $\mathcal{V}_{\hbar}^{\text{ск}}$;

$s_{\hbar}^{\text{к}}$ — конечная ситуация (состояние) на момент завершения выполнения $\mathcal{V}_{\hbar}^{\text{ск}}$;

$v_{\text{ƛ}}^{\hbar}$ — произвольная (ƛ) операция, образующая $\mathcal{V}_{\hbar}^{\text{ск}}$;

ℓ — общее количество $v_{\text{ƛ}}^{\hbar}$.

Для решения (1) определим $\mathcal{V}_{\hbar}^{\text{ск}}$, где $\hbar = \overline{1,3}$, представляющие собой частично упорядоченные последовательности операций ($\bigcup_{\text{ƛ}=1}^{\ell} v_{\text{ƛ}}^{\hbar}$), посредством применения метода Файкса, Харти и Нильсона [18, 19], в рамках которого построим треугольные таблицы по следующим правилам:

1. Количество строк и столбцов, образующих треугольную таблицу, равно $\ell+1$.

2. Строки нумеруются от 1 до $\ell+1$, а столбцы — от 0 до ℓ.

3. Каждый произвольный столбец ($\eth \geq 1$) треугольной таблицы помечается соответствующей $v_{\text{ƛ}}^{\hbar}$ и заполняется следующими результатами:

в столбце $\eth$ строке $\eth+1$ помещается результат выполнения соответствующей $v_{\text{ƛ}}^{\hbar}$ ($s_{\text{ƛ}}^{\hbar}$);

в столбце $\eth$ строке $\eth+ƀ$, где $ƀ = 2, 3, ...$, $\ell+1-\eth$, помещаются те результаты из $s_{\text{ƛ}}^{\hbar}$, кото-

рые сохраняются после последовательности соответствующих операций $v^{\hbar}_{\lambda+1}$, $v^{\hbar}_{\lambda+2}$, …, $v^{\hbar}_{\lambda+b-1}$. При этом, обозначим указанные результаты через $s^{\hbar}_{\lambda/\lambda+1\div\lambda+b-1}$.

4. В столбце 0 произвольной строке, номер которой соответствуют λ, треугольной таблицы помещаются начальные исходные данные ($s^{\hbar}_{0\lambda}$), которые должны быть в модели до выполнения соответствующей $v^{\hbar}_{\lambda}$, но которые еще не появились в соответствующей строке в результате выполнения операций, предшествующих $v^{\hbar}_{\lambda}$.

5. Исходные данные для $v^{\hbar}_{\lambda}$ помечаются "*".

Применяя вышеуказанные правила, зададим функцию определения интерпретатора скрипта для локального измерения значений ПД на СС СОПКА ($\Psi_1^{\text{ск}}$) (рис. 2) в виде стратегии, представленной на рис. 3.

В стратегии, представленной на рис. 3, приняты следующие обозначения: s^1_{01} — данные о стандартных интерпретаторах, предустановленных на СС СОПКА, отсутствуют; s^1_{02} — данные о современных и часто используемых ИЯ в наличии; s^1_{03} — ПД, описывающие типы СС СОПКА, получены; s^1_{04} — нормативные правовые акты, определяющие требования к программным средствам, применяемым для обеспечения безопасности объектов критической информационной инфраструктуры (КИИ), в наличии [1, 2, 5, 11]; s^1_{05} — данные о современных интерпретаторах в наличии; s^1_{06} — атрибуты ПД, описывающие эталонные образы СС СОПКА, получены; s^1_1, $s^1_{1/2\div2}$, $s^1_{1/2\div3}$, $s^1_{1/2\div4}$ — набор стандартных интерпретаторов, предустановленных на СС СОПКА, и соответствующие им ИЯ определены; s^1_2, $s^1_{2/3\div3}$, $s^1_{2/3\div4}$, $s^1_{2/3\div5}$, $s^1_{2/3\div6}$, $s^1_{2/3\div7}$, $s^1_{2/3\div8}$ — БДИЯ создана; s^1_3, $s^1_{3/4\div4}$, $s^1_{3/4\div5}$, $s^1_{3/4\div6}$, $s^1_{3/4\div7}$ — идентификаторы (типы (наименования) операционных систем, на базе которых развернуты объекты контроля) СС СОПКА получены; s^1_4, $s^1_{4/5\div5}$ — требования к программным средствам, применяемым для обеспечения безопасности объектов КИИ, определены; s^1_5, $s^1_{5/6\div6}$, $s^1_{5/6\div7}$, $s^1_{5/6\div8}$ — БДИ создана; s^1_6, $s^1_{6/7\div7}$, $s^1_{6/7\div8}$ — БД СБПК создана; s^1_7, $s^1_{7/8\div8}$ — ИЯ задан; s^1_8 — интерпретатор скрипта и файлы СБПК для локального измерения значений базовых атрибутов ПД, характеризующих состояние ПФ произвольного (g) СС, определены.

1	s^1_{01}*	v^1_1 — определить набор стандартных интерпретаторов на СС							
2	s^1_{02}*	s^1_1*	v^1_2 — сформировать БДИЯ						
3	s^1_{03}*	$s^1_{1/2\div2}$	s^1_2	v^1_3 — выделить идентификаторы СС					
4	s^1_{04}*	$s^1_{1/2\div3}$	$s^1_{2/3\div3}$	s^1_3	v^1_4 — сформировать множество требований к программным средствам КИИ				
5	s^1_{05}*	$s^1_{1/2\div4}$*	$s^1_{2/3\div4}$*	$s^1_{3/4\div4}$*	s^1_4*	v^1_5 — сформировать БДИ			
6	s^1_{06}*	∅	$s^1_{2/3\div5}$	$s^1_{3/4\div5}$	$s^1_{4/5\div5}$*	s^1_5*	v^1_6 — сформировать БД СБПК		
7	∅	∅	$s^1_{2/3\div6}$*	$s^1_{3/4\div6}$	∅	$s^1_{5/6\div6}$	s^1_6*	v^1_7 — выбрать ИЯ	
8	∅	∅	$s^1_{2/3\div7}$	$s^1_{3/4\div7}$*	∅	$s^1_{5/6\div7}$*	$s^1_{6/7\div7}$*	s^1_7*	v^1_8 — выбрать интерпретатор скрипта для g-го СС
9	∅	∅	$s^1_{2/3\div8}$	∅	∅	$s^1_{5/6\div8}$	$s^1_{6/7\div8}$	$s^1_{7/8\div8}$	s^1_8
	0	1	2	3	4	5	6	7	8

Рис. 3. Стратегия определения интерпретатора скрипта для локального измерения значений ПД на СС СОПКА

Исходя из (1) и стратегии определения интерпретатора скрипта (рис. 3) зададим $s_1^{\text{и}}$, $s_1^{\text{к}}$ и $\mathcal{V}_1^{\text{ск}}$ в виде [18, 19]:

$$s_1^{\text{и}} = \bigcup_{\tilde{\lambda}=1}^{6} s_{0\tilde{\lambda}}^1. \quad (2)$$

$$s_1^{\text{к}} = s_{2/3\div 8}^1 \bigcup s_{5/6\div 8}^1 \bigcup s_{6/7\div 8}^1 \bigcup s_{7/8\div 8}^1 \bigcup s_8^1. \quad (3)$$

$$\mathcal{V}_1^{\text{ск}} = v_1^1, \overset{\swarrow\ \nwarrow}{\underset{\searrow\ \nearrow}{v_2^1}}, \overset{\swarrow\ \nwarrow}{\underset{\searrow\ \nearrow}{v_3^1}}, \overset{\swarrow\ \nwarrow}{\underset{\searrow\ \nearrow}{v_4^1}}, v_5^1, v_6^1, v_7^1, v_8^1, \quad (4)$$

где $\swarrow$, $\searrow$, $\nearrow$, $\nwarrow$ — символы, обозначающие возможность перестановки $v_{\tilde{\lambda}}^{\hbar} \in \mathcal{V}_{\hbar}^{\text{ск}}$.

Далее определим функцию формирования ПБПК для локального измерения значений специфичных атрибутов ПД на СС СОПКА ($\mathcal{V}_2^{\text{ск}}$) (рис. 2) в виде стратегии, представленной на рис. 4.

В стратегии, представленной на рис. 4, приняты следующие обозначения: s_{01}^2 — множество файлов СБПК ($A_{w_{\partial}^{\text{итр}}}^{\text{фсбпк}}$), доступной для произвольного (∂) интерпретатора ($w_{\partial}^{\text{итр}}$), выбранного посредством v_8^1, определено и данные о глобальных и локальных переменных, используемых в произвольном (f) файле ($A_f^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$), содержащем описание общепринятой функции, применяемой для локального измерения значения определенного базового атрибута ПД на g-м СС, и включенным в СБПК, доступную для $w_{\partial}^{\text{итр}}$ ($\mathcal{F}_g^{\text{фсбпк/лизм}}$ — общее количество $A_f^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$), отсутствуют, либо не актуальны; s_{02}^2 — множества ($M_g^{\text{апд}}$) атрибутов ПД, описывающих эталонный образ g-го СС, и множество ($M_{w_{\partial}^{\text{итр}}}^{g^{\text{бапд}}}$) базовых атрибутов ПД, описывающих

1	s_{01}^2 *	v_1^2 — определить множества глобальных и локальных переменных, используемых в $A_f^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $f = \overline{1, \mathcal{F}_g^{\text{фсбпк/лизм}}}$						
2	s_{02}^2 *	s_1^2	v_2^2 — определить множество специфичных атрибутов ПД, описывающих эталонный образ g-го СС					
3	s_{03}^2 *	$s_{1/2\div 2}^2$	s_2^2	v_3^2 — сформировать множество требований надежного программирования				
4	s_{04}^2 *	$s_{1/2\div 3}^2$ *	$s_{2/3\div 3}^2$ *	s_3^2 *	v_4^2 — объявить глобальные и локальные переменные, используемые в инструкциях измерения значений специфичных атрибутов ПД на g-м СС			
5	s_{05}^2 *	∅	∅	$s_{3/4\div 4}^2$ *	s_4^2 *	v_5^2 — описать инструкции для доступа к местам хранения значений специфичных атрибутов ПД на g-м СС		
6	∅	∅	∅	$s_{3/4\div 5}^2$ *	$s_{4/5\div 5}^2$ *	s_5^2 *	v_6^2 — описать инструкции для считывания значений специфичных атрибутов ПД на g-м СС	
7	s_{07}^2 *	∅	∅	$s_{3/4\div 6}^2$ *	$s_{4/5\div 6}^2$ *	$s_{5/6\div 6}^2$	s_6^2 *	v_7^2 — описать инструкции действий в исключительных ситуациях при считывании значений специфичных атрибутов ПД на g-м СС
8	∅	∅	∅	∅	$s_{4/5\div 7}^2$ *	$s_{5/6\div 7}^2$ *	$s_{6/7\div 7}^2$ *	s_7^2 *	v_8^2 — сформировать БД ПБПК
9	∅	∅	∅	∅	$s_{4/5\div 8}^2$	$s_{5/6\div 8}^2$	$s_{6/7\div 8}^2$	$s_{7/8\div 8}^2$	s_8^2
	0	1	2	3	4	5	6	7	8

Рис. 4. Стратегия формирования ПБПК для локального измерения значений специфичных атрибутов ПД на СС СОПКА

эталонный образ g-го ИСИБ (СС), значения которых способен предоставлять $w_{\partial}^{\text{итр}}$ посредством использования $A_{w_{\partial}^{\text{итр}}}^{\text{фсбпк}}$, определены; s_{03}^2 — рекомендации, определяющие технологии и методы программирования, в наличии; s_{04}^2 — данные о резервной области памяти, необходимой для описания инструкций измерения значений специфичных атрибутов ПД на g-м СС, в наличии; s_{05}^2 — данные о местах хранения значений специфичных атрибутов ПД на g-м СС в наличии; s_{07}^2 — данные о возможных ошибках при считывании значений специфичных атрибутов ПД на g-м СС в наличии; s_1^2, $s_{1/2\div2}^2$, $s_{1/2\div3}^2$ — множества глобальных и локальных переменных, используемых в $A_f^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $f=\overline{1,\mathcal{F}_g^{\text{фсбпк/лизм}}}$, определены; s_2^2, $s_{2/3\div3}^2$ — множество специфичных атрибутов ПД, описывающих эталонный образ g-го СС, определено; s_3^2, $s_{3/4\div4}^2$, $s_{3/4\div5}^2$, $s_{3/4\div6}^2$ — требования надежного программирования определены; s_4^2, $s_{4/5\div5}^2$, $s_{4/5\div6}^2$, $s_{4/5\div7}^2$, $s_{4/5\div8}^2$ — набор глобальных и локальных переменных, используемых в инструкциях измерения значений специфичных атрибутов ПД на g-м СС, определен; s_5^2, $s_{5/6\div6}^2$, $s_{5/6\div7}^2$, $s_{5/6\div8}^2$ — набор инструкций доступа к местам хранения значений специфичных атрибутов ПД на g-м СС определен; s_6^2, $s_{6/7\div7}^2$, $s_{6/7\div8}^2$ — набор инструкций считывания значений специфичных атрибутов ПД на g-м СС определен; s_7^2, $s_{7/8\div8}^2$ — набор инструкций, задающих порядок действий в исключительных ситуациях при считывании значений специфичных атрибутов ПД на g-м СС, определен; s_8^2 — БД ПБПК создана.

Поясним отдельные аспекты стратегии формирования ПБПК (рис. 4):

1. Начальные исходные данные s_{01}^2, в части касающейся не актуальности данных о глобальных и локальных переменных, используемых в $A_f^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $f=\overline{1,\mathcal{F}_g^{\text{фсбпк/лизм}}}$, свидетельствуют о возможном периодическом увеличении значения $\mathcal{F}_g^{\text{фсбпк/лизм}}$, что необходимо учитывать при выполнении v_1^2.

2. Начальные исходные данные s_{03}^2, s_{04}^2, s_{05}^2, s_{07}^2 определяются специалистом по информационной безопасности (ИБ) на основе собственного опыта и существующих передовых практик в заданной предметной области [10, 15, 16], в связи с чем они не указываются на диаграмме "Синтезировать скрипт для локального измерения значений ПД на СС СОПКА" (рис. 1, 2).

3. Множество $M_g^{\text{апд}}$ задается специалистом по ИБ на этапе подготовки к эксплуатации САК посредством модуля ее настройки [6] с учетом данных о заданных режимах функционирования g-го СС. При этом отметим, что $M_{w_{\partial}^{\text{итр}}}^{g^{\text{бапд}}} \subset M_g^{\text{апд}}$, $A_{w_{\partial}^{\text{итр}}}^{\text{фсбпк}} \triangleq M_{w_{\partial}^{\text{итр}}}^{g^{\text{бапд}}}$.

4. Под переменной понимаем именованный идентификатор, обозначающий некоторую область памяти, используемую в инструкциях, образующих скрипт для локального измерения значений ПД на СС СОПКА [16].

На основе (1) и стратегии формирования ПБПК (рис. 4) определим $s_2^{\text{и}}$, $s_2^{\text{к}}$ и $\mathcal{V}_2^{\text{ск}}$ в виде [18, 19]:

$$s_2^{\text{и}} = s_{01}^2 \cup s_{02}^2 \cup s_{03}^2 \cup s_{04}^2 \cup s_{05}^2 \cup s_{07}^2. \quad (5)$$

$$s_2^{\text{к}} = s_{4/5\div8}^2 \cup s_{5/6\div8}^2 \cup s_{6/7\div8}^2 \cup s_{7/8\div8}^2 \cup s_8^2. \quad (6)$$

$$\mathcal{V}_2^{\text{ск}} = \overset{\swarrow\ \nwarrow\swarrow\ \nwarrow}{v_1^2, v_2^2, v_3^2, v_4^2, v_5^2, v_6^2, v_7^2, v_8^2}. \quad (7)$$
$$\searrow\ \nearrow\searrow\ \nearrow$$

В дополнение к (7), поясним отдельные операции, образующие $\mathcal{V}_2^{\text{ск}}$:

1. Необходимость операции v_1^2 обусловлена тем, что при выполнении общепринятой функции, описанной в $A_f^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $f=\overline{1,\mathcal{F}_g^{\text{фсбпк/лизм}}}$, используемые в ней переменные располагаются в некоторых областях памяти (локальная и глобальная), характеризующихся разным периодом существования, и инициализируются определенными значениями. При этом значения переменных, используемых в $A_f^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$ и располагающихся в глобальной области памяти, могут быть использованы при описании уникальных функций, обеспечивающих локальное измерение значений специфичных атрибутов ПД на g-м СС.

2. Операции $v_3^2 - v_7^2$ реализуются специалистом по ИБ на основе исходных данных, указанных на рис. 4, и путем применения ИЯ, выбранного посредством v_7^1, своевременно и в объеме, обеспечивающем достижение целей выполнения $\mathcal{V}_2^{\text{ск}}$ [15, 16].

3. Операция v_8^2 заключается в автоматическом формировании произвольного (g) файла, содержащего описание уникальной функции, обеспечивающей локальное измерение значения определенного специфичного атрибута ПД на g-м СС ($A_g^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фпбпк}}} \in A_{w_\partial^{\text{итр}}}^{\text{фпбпк}}$, $g=\overline{1,\mathcal{F}_g^{\text{фпбпк/лизм}}}$, где $A_{w_\partial^{\text{итр}}}^{\text{фпбпк}}$ — множество файлов ПБПК, доступной для $w_\partial^{\text{итр}}$; $\mathcal{F}_g^{\text{фпбпк/лизм}}$ — общее количество $A_g^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фпбпк}}}$), с последующим сохранением его в БД ПБПК. При этом отметим, что $A_g^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фпбпк}}}$ состоит из упорядоченного набора соответствующих инструкций, получаемых в результате последовательного выполнения $v_4^2 - v_7^2$ (рис. 4).

Кроме того, определим функцию формирования образа скрипта для локального измерения значений базовых и специфичных атрибутов ПД на СС СОПКА ($\lambda_3^{\text{ск}}$) (рис. 2) в виде стратегии, представленной на рис. 5, на котором приняты следующие обозначения: s_{01}^3 — данные о заданных режимах функционирования СС СОПКА в наличии и $A_{w_\partial^{\text{итр}}}^{\text{фсбпк}}$ сформировано; s_{02}^3 — данные о текущем режиме функционирования g-го СС в наличии; s_{03}^3 — данные о наименовании $w_\partial^{\text{итр}}$, $A_f^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $f=\overline{1,\mathcal{F}_g^{\text{фсбпк/лизм}}}$, $A_g^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фпбпк}}}$, $g=\overline{1,\mathcal{F}_g^{\text{фпбпк/лизм}}}$, а также о наименовании и типах базовых и специфичных атрибутов ПД g-го СС, значения которых предоставляются посредством указанных файлов, в наличии; s_{04}^3 — данные о переменных, используемых в $A_f^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $f=\overline{1,\mathcal{F}_g^{\text{фсбпк/лизм}}}$, $A_g^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фпбпк}}}$, $g=\overline{1,\mathcal{F}_g^{\text{фпбпк/лизм}}}$, в наличии; s_{05}^3 — данные о наборах инструкций локального измерения, описанных в $A_f^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $f=\overline{1,\mathcal{F}_g^{\text{фсбпк/лизм}}}$, $A_g^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фпбпк}}}$, $g=\overline{1,\mathcal{F}_g^{\text{фпбпк/лизм}}}$, в наличии; s_{08}^3 — данные о возможных ошибках во входных данных $\mathfrak{I}_g^\zeta$ и при выполнении функций, описанных в $A_f^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$ и $A_\eta^{w_\partial^{\text{итр}}/\zeta_{\text{прч}}^{\text{фсбпк}}}$, а также требования надежного программирования в наличии; s_1^3, $s_{1/2\div2}^3$, $s_{1/2\div3}^3$, $s_{1/2\div4}^3$, $s_{1/2\div5}^3$, $s_{1/2\div6}^3$ — множество $A_{w_\partial^{\text{итр}}}^{\text{фсбпк/оп}}$ сформировано; s_2^3 — текущий режим функционирования g-го СС определен; s_3^3, $s_{3/4\div4}^3$, $s_{3/4\div5}^3$, $s_{3/4\div6}^3$, $s_{3/4\div7}^3$, $s_{3/4\div8}^3$, $s_{3/4\div9}^3$ — набор инструкций, указывающих на наименования $w_\partial^{\text{итр}}$, $A_f^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $A_\zeta^{w_\partial^{\text{итр}}/\zeta_{\text{обр}}^{\text{фсбпк}}}$, $A_\eta^{w_\partial^{\text{итр}}/\zeta_{\text{прч}}^{\text{фсбпк}}}$, в $\mathfrak{I}_g^\zeta$ включен и требуемые файлы $A_g^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фпбпк}}}$ определены; s_4^3, $s_{4/5\div5}^3$, $s_{4/5\div6}^3$, $s_{4/5\div7}^3$, $s_{4/5\div8}^3$, $s_{4/5\div9}^3$ — набор инициализированных переменных, используемых в $A_f^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $A_g^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фпбпк}}}$, $A_\zeta^{w_\partial^{\text{итр}}/\zeta_{\text{обр}}^{\text{фсбпк}}}$, $A_\eta^{w_\partial^{\text{итр}}/\zeta_{\text{прч}}^{\text{фсбпк}}}$, в $\mathfrak{I}_g^\zeta$ включен; s_5^3, $s_{5/6\div6}^3$, $s_{5/6\div7}^3$, $s_{5/6\div8}^3$, $s_{5/6\div9}^3$ — набор инструкций, описанных в $A_f^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $A_g^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фпбпк}}}$, в $\mathfrak{I}_g^\zeta$ включен; s_6^3, $s_{6/7\div7}^3$, $s_{6/7\div8}^3$, $s_{6/7\div9}^3$ — набор инструкций, описанных в $A_\zeta^{w_\partial^{\text{итр}}/\zeta_{\text{обр}}^{\text{фсбпк}}}$, в $\mathfrak{I}_g^\zeta$ включен; s_7^3, $s_{7/8\div8}^3$, $s_{7/8\div9}^3$ — набор инструкций, описанных в $A_\eta^{w_\partial^{\text{итр}}/\zeta_{\text{прч}}^{\text{фсбпк}}}$, в $\mathfrak{I}_g^\zeta$ включен; s_8^3, $s_{8/9\div9}^3$ — набор инструкций, задающих порядок действий в исключительных ситуациях при выполнении функций, описанных в $A_f^{w_\partial^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$ и $A_\eta^{w_\partial^{\text{итр}}/\zeta_{\text{прч}}^{\text{фсбпк}}}$, в $\mathfrak{I}_g^\zeta$ включен; s_9^3 — $\mathfrak{I}_g^\zeta$ сконфигурирован; $A_{w_\partial^{\text{итр}}}^{\text{фсбпк/оп}}$ — множество файлов, доступных для $w_\partial^{\text{итр}}$ и содержащих описания общепринятых функций, обеспечивающих обработку и передачу локально измеренных значений базовых и специфичных атрибутов ПД на СС в адрес ППК САК [6]; $\mathfrak{I}_g^\zeta$ — образ скрипта для локального измерения значений ПД на g-м СС в произвольном (ζ) режиме его функционирования; $A_\zeta^{w_\partial^{\text{итр}}/\zeta_{\text{обр}}^{\text{фсбпк}}}$, $A_\eta^{w_\partial^{\text{итр}}/\zeta_{\text{прч}}^{\text{фсбпк}}}$ — произвольные (ζ, η) файлы, соответственно содержащие описания общепринятых функций, используемых в ζ-м режиме функционирования СС СОПКА для обработки и передачи локально измеренных значений базовых и специфичных атрибутов ПД на объектах контроля в адрес средства контроля [6].

Отметим некоторые аспекты стратегии формирования $\mathfrak{I}_g^\zeta$ (рис. 5):

1. Начальные исходные данные s_{01}^3, s_{02}^3, за исключением формирования $A_{w_\partial^{\text{итр}}}^{\text{фсбпк}}$, задаются специалистом по ИБ соответственно на этапах подготовки и непосредственной эксплуатации САК посредством модуля ее настройки [6].

2. Источниками начальных исходных данных s_{03}^3, s_{04}^3, s_{05}^3 являются БД СБПК и БД ПБПК, формируемые посредством v_6^1 и v_8^2.

3. Начальные исходные данные s_{08}^3, в части касающейся требований надежного программирования, определяются посредством v_3^2, а в остальном — специалистом по ИБ на основе вышеуказанных пояснений отдельных аспектов стратегии формирования ПБПК.

4. Под обработкой локально измеренных значений базовых и специфичных атрибутов ПД на объектах контроля понимаем процедуру приведения соответствующих значений к определенному формату, пригодному для их передачи в ППК САК [6].

5. Под передачей локально измеренных и обработанных значений базовых и специфичных атрибутов ПД на объектах контроля понимаем процедуру установления сетевого взаимодействия СС с ППК САК [6] и отправки в ее адрес соответствующих значений ПД в определенном порядке.

Далее, учитывая (1) и стратегию формирования $\mathfrak{I}_g^{\zeta}$ (рис. 5), определим $s_3^{\text{и}}$, $s_3^{\text{к}}$, $\mathcal{V}_3^{\text{ск}}$ в виде [18, 19]:

$$s_3^{\text{и}} = s_{01}^3 \bigcup s_{02}^3 \bigcup s_{03}^3 \bigcup s_{04}^3 \bigcup s_{05}^3 \bigcup s_{08}^3. \tag{8}$$

$$s_3^{\text{к}} = s_{3/4\div9}^3 \bigcup s_{4/5\div9}^3 \bigcup s_{5/6\div9}^3 \bigcup s_{6/7\div9}^3 \bigcup s_{7/8\div9}^3 \bigcup \bigcup s_{8/9\div9}^3 \bigcup s_9^3. \tag{9}$$

$$\mathcal{V}_3^{\text{ск}} = \overset{\swarrow\ \nwarrow}{v_1^3, v_2^3, v_3^3, v_4^3, v_5^3, v_6^3, v_7^3, v_8^3, v_9^3}\ \underset{\searrow\ \nearrow}{} \tag{10}$$

1	s_{01}^3*	v_1^3 — сформировать $A_{w_{\partial}^{\text{итр}}}^{\text{фсбпк/оп}} \subset A_{w_{\partial}^{\text{итр}}}^{\text{фсбпк}}$							
2	s_{02}^3*	s_1^3	v_2^3 — определить текущий режим функционирования g-го СС						
3	s_{03}^3*	$s_{1/2\div2}^3$*	s_2^3*	v_3^3 — включить в $\mathfrak{I}_g^{\zeta}$ указатели на наименования $w_{\partial}^{\text{итр}}$, $A_f^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $A_{\nearrow}^{w_{\partial}^{\text{итр}}/\zeta_{\text{обр}}^{\text{фсбпк}}}$, $A_{\nwarrow}^{w_{\partial}^{\text{итр}}/\zeta_{\text{прч}}^{\text{фсбпк}}}$ и определить требуемые $A_g^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фпбпк}}}$					
4	s_{04}^3*	$s_{1/2\div3}^3$*	∅	s_3^3*	v_4^3 — включить в $\mathfrak{I}_g^{\zeta}$ переменные, используемые в $A_f^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $A_g^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фпбпк}}}$, $A_{\nearrow}^{w_{\partial}^{\text{итр}}/\zeta_{\text{обр}}^{\text{фсбпк}}}$, $A_{\nwarrow}^{w_{\partial}^{\text{итр}}/\zeta_{\text{прч}}^{\text{фсбпк}}}$, и инициализировать их				
5	s_{05}^3*	$s_{1/2\div4}^3$	∅	$s_{3/4\div4}^3$*	s_4^3*	v_5^3 — включить в $\mathfrak{I}_g^{\zeta}$ функции, описанные в $A_f^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $A_g^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фпбпк}}}$				
6	∅	$s_{1/2\div5}^3$*	∅	$s_{3/4\div5}^3$*	$s_{4/5\div5}^3$*	s_5^3*	v_6^3 — включить в $\mathfrak{I}_g^{\zeta}$ функцию, описанную в $A_{\nearrow}^{w_{\partial}^{\text{итр}}/\zeta_{\text{обр}}^{\text{фсбпк}}}$			
7	∅	$s_{1/2\div6}^3$*	∅	$s_{3/4\div6}^3$*	$s_{4/5\div6}^3$*	$s_{5/6\div6}^3$	s_6^3*	v_7^3 — включить в $\mathfrak{I}_g^{\zeta}$ функцию, описанную в $A_{\nwarrow}^{w_{\partial}^{\text{итр}}/\zeta_{\text{прч}}^{\text{фсбпк}}}$	
8	s_{08}^3*	∅	∅	$s_{3/4\div7}^3$	$s_{4/5\div7}^3$*	$s_{5/6\div7}^3$*	$s_{6/7\div7}^3$	s_7^3*	v_8^3 — описать и включить в $\mathfrak{I}_g^{\zeta}$ инструкции действий в исключительных ситуациях при выполнении функций, описанных в $A_f^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$ и $A_{\nwarrow}^{w_{\partial}^{\text{итр}}/\zeta_{\text{прч}}^{\text{фсбпк}}}$
9	∅	∅	∅	$s_{3/4\div8}^3$*	$s_{4/5\div8}^3$*	$s_{5/6\div8}^3$*	$s_{6/7\div8}^3$*	$s_{7/8\div8}^3$*	s_8^3*	v_9^3 — сконфигурировать $\mathfrak{I}_g^{\zeta}$
10	∅	∅	∅	$s_{3/4\div9}^3$	$s_{4/5\div9}^3$	$s_{5/6\div9}^3$	$s_{6/7\div9}^3$	$s_{7/8\div9}^3$	$s_{8/9\div9}^3$	s_9^3
	0	1	2	3	4	5	6	7	8	9

Рис. 5. Стратегия формирования образа скрипта для локального измерения значений базовых и специфичных атрибутов ПД на СС СОПКА

Дополняя (10), поясним отдельные операции, образующие $\mathcal{V}_3^{\text{ск}}$:

1. Необходимость операции v_2^3 обусловлена тем, что интенсивность и сложность компьютерных атак на ПФ СОПКА в ζ-х режимах ее функционирования разная, в связи с чем целесообразно задавать определенное количество контролируемых атрибутов ПД, характеризующих состояние ПФ объекта контроля, последовательность локального измерения их значений, а также определять конкретные $A_{\dot{\imath}}^{w_{\partial}^{\text{итр}}/\zeta_{\text{обр}}^{\text{фсбпк}}}$ и $A_{\dot{\eta}}^{w_{\partial}^{\text{итр}}/\zeta_{\text{прч}}^{\text{фсбпк}}}$ [20—22]. При этом, операция v_2^3 реализуется посредством автоматического запроса из модуля настройки САК [6] соответствующих исходных данных, указанных на рис. 5, и формирования вывода о ζ-м режиме функционирования g-го СС.

2. Операции $v_3^3 - v_8^3$ реализуются посредством автоматического запроса из БД СБПК и БД ПБПК соответствующих исходных данных, указанных на рис. 5, и упорядоченного размещения результатов их выполнения в $\mathfrak{I}_g^{\zeta}$.

3. Операция v_4^3, в части касающейся инициализации переменных, используемых в $A_f^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$, $A_g^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фпбпк}}}$, $A_{\dot{\imath}}^{w_{\partial}^{\text{итр}}/\zeta_{\text{обр}}^{\text{фсбпк}}}$, $A_{\dot{\eta}}^{w_{\partial}^{\text{итр}}/\zeta_{\text{прч}}^{\text{фсбпк}}}$, и операция v_8^3, в части касающейся описания инструкций действий в исключительных ситуациях при выполнении функций, описанных в $A_f^{w_{\partial}^{\text{итр}}/g_{\text{лизм}}^{\text{фсбпк}}}$ и $A_{\dot{\eta}}^{w_{\partial}^{\text{итр}}/\zeta_{\text{прч}}^{\text{фсбпк}}}$, реализуются специалистом по ИБ на основе исходных данных, указанных на рис. 5, и путем применения ИЯ, выбранного посредством v_7^1, своевременно и в объеме, обеспечивающем достижение целей выполнения $\mathcal{V}_3^{\text{ск}}$ [15, 16].

4. Операция v_9^3 реализуется посредством автоматического задания структуры конфигурации $\mathfrak{I}_g^{\zeta}$ в виде упорядоченного набора соответствующих инструкций, получаемых в результате последовательного выполнения $v_3^3 - v_8^3$ (рис. 5).

Заключение

В завершении отметим, что дальнейшим направлением исследования является разработка формализованных описаний отдельных операций, выделенных в функциональной модели синтеза скрипта контроля состояния ПФ СОПКА, а также построение на их основе соответствующей программной модели, предоставляющей возможность практической реализации ППК САК [6], обеспечивающей повышение оперативности процесса контроля состояния ПФ СОПКА, функционирующей в условиях часто появляющихся фактов НСВ с САК [6], посредством структуризации и автоматизации отдельных операций, реализуемых специалистом по ИБ на этапе подготовки и непосредственной эксплуатации модуля локального измерения типа, состояния ПФ СОПКА и ее условий эксплуатации.

Литература

1. Приказ Федеральной службы по техническому и экспортному контролю России от 21 декабря 2017 года № 235 "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования" [Электронный ресурс]. Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1589-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-236.

2. Приказ Федеральной службы по техническому и экспортному контролю России от 25 декабря 2017 года № 239 "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" [Электронный ресурс]. Режим доступа: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239.

3. *Коноваленко С. А., Королев И. Д., Секунов В. Г.* Моделирование системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Информационные системы и технологии. 2022. № 1(129). С. 105—113.

4. ГОСТ Р ИСО/МЭК 25010-2015. Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модель качества систем и программных продуктов. — М.: Стандартинформ, 2015. — 36 с.

5. Приказ Федеральной службы безопасности Российской Федерации от 6 мая 2019 года № 196 "Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты" [Электронный ресурс]. Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201905310017.

6. *Коноваленко С. А.* Модель адаптивного контроля системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Информация и безопасность. 2022. Т. 25. № 1. С. 141—154.

7. *Минаев В. А., Королев И. Д., Мазин А. В., Коноваленко С. А.* Модель выявления уязвимостей при нестабильных сетевых взаимодействиях с автоматизированной системой // Радиопромышленность. 2018. № 2. С. 48—57.

8. *Коноваленко С. А., Королев И. Д., Стадник А. Н., Маркин Д. И., Рогозин Е. А., Васильев Д. С.* Способ комбинированного контроля состояния процесса функционирования автоматизированных систем: пат. 2758974 Рос. Федерация / заявитель, патентообладатель Федеральное государственное казенное военное образовательное учреждение высшего образования "Краснодарское высшее военное училище им. генерала армии С. М. Штеменко", МО РФ. — № 2021106246, заявл. 10.03.2021, опубл. 03.11.2021, Бюл. № 31. — 57 с.

9. *Коноваленко С. А., Королев И. Д., Максимов Р. В., Симонов А. В.* Способ мониторинга безопасности автоматизированных систем: пат. 2646388 Рос. Федерация / заявитель, патентообладатель Федеральное государственное казенное военное образовательное учреждение высшего образования "Краснодарское высшее военное училище им. генерала армии С. М. Штеменко", МО РФ. — № 2017114327, заявл. 24.04.2017, опубл. 02.03.2018, Бюл. № 7. — 22 с.

10. ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. — М.: Стандартинформ, 2016. — 24 с.

11. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. — М.: Стандартинформ, 2006. — 62 с.

12. Методология функционального моделирования IDEF0. — М.: Госстандарт России, 2000. — 75 с.

13. ГОСТ Р 56920-2016. Системная и программная инженерия. Тестирование программного обеспечения. Часть 1. Понятия и определения. — М.: Стандартинформ, 2016. — 53 с.

14. *Борковской А. Б.* Англо-русский словарь по программированию и информатике (с толкованием). — М.: Рус. яз., 1990. С. 140.

15. *Пратт Т., Зелковиц М.* Языки программирования: разработка и реализация / под общей ред. А. Матросова. — Спб.: Питер, 2002. — 688 с.

16. *Макконнелл С.* Совершенный код. Мастер-класс / пер. с англ. — М.: Издательство "Русская редакция", 2010. — 896 с.

17. ГОСТ 28195-89. Оценка качества программных средств. Общие положения. — М.: ИПК Издательство стандартов, 1989. — 31 с.

18. *Ефимов Е. И.* Решатели интеллектуальных задач. — М.: Наука, Главная редакция физико-математической литературы, 1982. — 320 с.

19. *Хант Э.* Искусственный интеллект / под ред. В. Л. Стефанюка. пер. с англ. — М.: Мир, 1978. — 559 с.

20. *Безкоровайный М. М.,* Татузов *А. Л.* Кибербезопасность — подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1(2). С. 22—27.

21. *Белоус А. И., Солодуха В. А.* Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. — М.: ТЕХНОСФЕРА, 2021. С. 85—131.

22. Методический документ. Методика оценки угроз безопасности информации [утвержден Федеральной службой по техническому и экспортному контролю России 5 февраля 2021 г.]. — М.: ФСТЭК России, 2021. — 83 с.

The functional script synthesizing model for monitoring a system for detecting, preventing and eliminating the consequences of computer attacks

S. A. Konovalenko
Krasnodar Higher Military School named after Army General S. M. Shtemenko, Krasnodar, Russia

Based on the IDEF0 methodology, the article developed a functional script synthesizing model for local measurement of parametric data values characterizing the state of the process of functioning of the system for detecting, preventing and eliminating the consequences of computer attacks (SOPKA). The functional script synthesizing model for monitoring of the SOPKA includes many functions, the definition of which is carried out in the form of strategies presented by means of triangular tables, consisting of partially ordered sequences of selected operations, which provide the possibility of increasing the efficiency of the process of monitoring the state of the SOPKA operating in various modes and operating conditions.

Keywords: control, script, system for detecting, preventing and eliminating the consequences of computer attacks.

Bibliography — 22 references. *Received May 23, 2022*

УДК 003.26
DOI: 10.52190/2073-2600_2022_2_13
EDN: JEFCMK

Алгебраические алгоритмы со скрытой группой над конечными полями характеристики два

А. А. Курышева; *А. А. Костина*; *Н. А. Молдовян*, д-р техн. наук
Санкт-Петербургский федеральный исследовательский центр РАН (СПб ФИЦ РАН),
Санкт-Петербург, Россия

Рассмотрены особенности реализации алгоритмов ЭЦП на конечных некоммутативных ассоциативных алгебрах, заданных над конечными полями характеристики два. Интерес к реализациям данного типа связан с возможностью повышения производительности алгоритмов со скрытой группой, а также тем, что последние основаны на вычислительной трудности решения систем квадратных уравнений и для них является некритичным факторизация порядка скрытой группы. Последнее позволяет использовать поля $GF(2^z)$ не только со значениями степени расширения z, равной степени Мерсенна, но и при других значениях z. В качестве алгебраического носителя алгоритмов рассмотрены алгебры, заданные по прореженным таблицам умножения базисных векторов, и установлены основные типы коммутативных групп, содержащихся в таких алгебрах и представляющих интерес для использования в качестве скрытой группы.

Ключевые слова: информационная безопасность, цифровая подпись, постквантовая криптография, конечная ассоциативная алгебра, некоммутативная алгебра, скрытая группа.

Одним из актуальных современных вызовов в области прикладной и теоретической криптографии является разработка практичных постквантовых алгоритмов электронной цифровой подписи (ЭЦП), т. е. алгоритмов стойких к атакам с использованием обычных и квантовых компьютеров (квантовые атаки). Для последних известны полиномиальные алгоритмы решения задач факторизации (ЗФ) и дискретного логарифмирования (ЗДЛ) [1, 2], поэтому постквантовые алгоритмы ЭЦП должны основываться на других типах вычислительно трудных задач.

Для разработки практичных постквантовых алгоритмов ЭЦП ранее предложен подход, основанный на вычислительной сложности скрытой ЗДЛ [3, 4] и связанный с использованием конечных некоммутативных ассоциативных алгебр (КНАА). В алгоритмах данного типа используется секретная скрытая группа, в которой выполняются операции экспоненцирования при формировании открытого ключа и генерации ЭЦП, которые приводят к заданию скрытой ЗДЛ как базового криптографического примитива. Недавно предложен новый подход к построению алгоритмов ЭЦП со скрытой группой [5], который привел к новой концепции построения алгоритмов ЭЦП со скрытой группой [6], в которой сохранены технические приемы их построения, однако, изменен базовый примитив, которым стала вычислительная трудность решения систем из многих квадратных уравнений с многими неизвестными. В новой концепции на исходном этапе устраняется проблема обоснования стойкости к квантовым атакам, поскольку для решения указанных систем квантовый компьютер не является эффективным [7, 8]. При этом алгоритмы ЭЦП со скрытой группой, построенные на ее основе сопоставимы по производительности и достаточно малым размерам открытого ключа и подписи со схемами ЭЦП, основанными на скрытой ЗДЛ.

Для повышения производительности алгебраических алгоритмов со скрытой группой можно использовать в качестве алгебраического носителя КНАА, заданные по прореженным таблицам умножения базисных векторов (ТУБВ) [9]. Ранее рассматривался главным образом вариант использования КНАА заданных над простыми полями

Курышева Алена Андреевна, аспирант.
E-mail: kurysheva.al@yandex.ru
Костина Анна Александровна, научный сотрудник.
E-mail: anya@hotbox.ru
Молдовян Николай Андреевич, профессор, главный научный сотрудник.
E-mail: nmold@mail.ru

Статья поступила в редакцию 29 января 2022 г.

$GF(p)$ нечетной характеристики p [10—12]. Дополнительное повышение производительности алгоритмов ЭЦП и снижение схемотехнической сложности их реализации может быть обеспечено использованием КНАА заданных над конечными полями характеристики два.

В данной статье рассматриваются особенности использования КНАА, заданных над конечными полями характеристики два, в качестве алгебраического носителя алгоритмов ЭЦП со скрытой группой.

Задание КНАА

Конечные m-мерные алгебры задаются как конечное m-мерное векторное пространство с дополнительно определенной замкнутой операцией умножения всевозможных пар векторов, которая является обладает свойством дистрибутивности слева и справа относительно операции сложения. В данной статье рассматривается вариант задания алгебр над конечными полями $GF(2^z)$, элементами которых являются всевозможные двоичные многочлены степени не выше $z-1$, а операцией умножения — умножение двоичных многочленов по модулю неприводимого двоичного многочлена степени z. Элемент алгебры $\mathbf{A}$ можно представить в виде упорядоченного набора его координат $a_i \in GF(2^z)$, т. е. в виде $\mathbf{A} = (a_0, a_1, \ldots, a_{m-1})$, или в виде суммы его компонент $a_i\mathbf{e}_i$, т. е. в виде $\mathbf{A} = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$, где $\mathbf{e}_i$ — базисные векторы.

Операцию умножения векторов $\mathbf{A}$ и $\mathbf{B} = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ обычно задают по правилу перемножения каждой компоненты вектора $\mathbf{A}$ с каждой компонентой вектора $\mathbf{B}$:

$$\mathbf{AB} = \sum_{i,j=0}^{m-1} a_i b_j \left(\mathbf{e}_i\mathbf{e}_j\right),$$

где умножение координат выполняется в поле $GF(2^z)$, а всевозможные произведения пар базисных векторов $\mathbf{e}_i\mathbf{e}_j$ заменяются на соответствующие однокомпонентные векторы вида $\lambda\mathbf{e}_k$ (λ — структурная константа), указанные в ячейках на пересечении i-й строки и j-го столбца в некоторой специально составленной ТУБВ. Если заданная операция умножения обладает свойством некоммутативности и ассоциативности, то имеем КНАА.

Как правило, известные ТУБВ для задания КНАА над конечными простыми полями $GF(p)$ нечетной характеристики p также могут быть использованы для задания КНАА над полями $GF(2^z)$. Исключение составляют ТУБВ, в которых свойство некоммутативности обеспечивается не несимметричностью (относительно главной диагонали таблицы, проходящей из верхнего левого угла в нижний правый угол) распределения базисных векторов, а несимметричностью распределения структурного коэффициента, равного значению -1. Примерами последнего типа является ТУБВ, задающая конечную алгебру кватернионов [13], и ТУБВ из статей [14, 15]. В целом, имеются различные многообразные способы задания КНАА над конечными полями характеристики два, в том числе могут быть применены способы унифицированного задания КНАА [11, 16] различных четных размерностей (способы построения ТУБВ, выражаемые единой математической формулой, включающей значение размерности m в качестве параметра).

Для построения производительных алгоритмов ЭЦП со скрытой группой представляют интерес четырехмерные прореженные ТУБВ [16, 17], например ТУБВ, представленная как табл. 1. Свойства КНАА над простым конечным полем $GF(p)$ (при нечетном p) с операцией умножения, заданной по табл. 1, изучены в работе [17]. Все свойства, представленные в [17] переносятся на случай задания алгебры над полем $GF(2^z)$. Для дальнейшего представляют интерес следующие положения:

1. Алгебра, заданная по табл. 1, содержит глобальную двухстороннюю единицу в виде вектора $\mathbf{E} = (\mu^{-1}, \lambda^{-1}, 0, 0)$.

2. Условием обратимости вектора $\mathbf{A} = (a_0, a_1, a_2, a_3)$ является выполнимость неравенства $a_0a_1 \neq a_2a_3$.

3. Порядок мультипликативной группы алгебры равен значению $\Omega = 2^z(2^z - 1)(2^{2z} - 1)$.

4. Векторы вида $\mathbf{L} = (\sigma\mu^{-1}, \sigma\lambda^{-1}, 0, 0)$ при всевозможных $\sigma \in GF(2^z)$ являются скалярными векторами (скалярным называется вектор $\mathbf{L}$, такой, что для любого вектора $\mathbf{V}$ выполняется соотношение $\mathbf{LV} = \mathbf{VL} = \sigma\mathbf{V}$ для некоторого скалярного значения σ).

Таблица 1

Задание операции умножения четырехмерной КНАА ($\mu, \lambda \in GF(2^z)$; $\mu \neq 0$; $\lambda \neq 0$) [17]

•	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mu\mathbf{e}_0$	0	0	$\mu\mathbf{e}_3$
$\mathbf{e}_1$	0	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	0
$\mathbf{e}_2$	$\mu\mathbf{e}_2$	0	0	$\mu\mathbf{e}_1$
$\mathbf{e}_3$	0	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_0$	0

Основные типы коммутативных групп

При построении алгоритмов ЭЦП со скрытой группой важным является строение КНАА, ис-

пользуемой в качестве алгебраического носителя, с точки зрения разбиения на коммутативные подалгебры. Способ изучения строения КНАА, заданных над полем $GF(p)$ [16], в целом может быть применен и для КНАА, заданной по табл. 1 над полем $GF(2^z)$. Выполненное рассмотрение строения КНАА для последнего случая показало следующее:

1. Четырехмерная КНАА заданная по табл. 1 над полем $GF(2^z)$, разбивается на коммутативные подалгебры порядка 2^{2z}, попарно пересекающиеся строго в множестве скалярных векторов.

2. Коммутативные подалгебры относятся к трем различным типам, отличающимся строением их мультипликативной группы.

3. Три типа коммутативных подалгебр задают существование в КНАА следующих трех различных типов коммутативных групп:

3.1) коммутативные группы с двухмерной цикличностью (группы с двумя образующими одинакового порядка [18, 19]), порядок которых равен значению $\Omega_1 = (2^z - 1)^2$;

3.2) циклические коммутативные группы, порядок которых равен значению $\Omega_2 = 2^{2z} - 1$;

3.3) циклические коммутативные группы, порядок которых равен значению $\Omega_3 = 2^z(2^z - 1)$;

В алгоритмах ЭЦП со скрытой группой в качестве последней представляет интерес использование коммутативных групп с двухмерной цикличностью. Выбор случайной группы такого типа задается при формировании секретного ключа как генерация двух случайных векторов **G** и **H** порядка $2^z - 1$, образующих ее базис (минимальную систему образующих группы).

Генерация базиса <**G**, **H**> группы с двухмерной цикличностью может быть выполнена по следующему алгоритму:

1. Сгенерировать случайный вектор **R** порядка $2^z - 1$.

2. Если **R** является скалярным вектором, то перейти к шагу 1.

3. Сгенерировать случайный двоичный многочлен $\rho \in GF(2^z)$ порядка $2^z - 1$.

4. Сгенерировать случайное число k $(1 < k < 2^z - 1)$ и вычислить вектор $\mathbf{H} = \rho\mathbf{R}^k$.

5. Взять в качестве базиса группы пару векторов **G** = **R** и **H**.

Сравнение двух типов алгоритмов ЭЦП со скрытой группой

Алгоритмы (схемы) ЭЦП, стойкость которых основана на вычислительной трудности скрытой ЗДЛ, будем называть алгоритмами (схемами ЭЦП) первого типа. Соответственно ко второму типу будем относить алгоритмы (схемы ЭЦП), стойкость которых основана на вычислительной трудности решения системы из многих квадратных уравнений с многими неизвестными.

Рассмотрим основные элементы сходства:

1. Схемы ЭЦП обоих типов относятся к алгебраическим криптосхемам, т. е. в качестве их алгебраического носителя используются конечные алгебры, а более точно, КНАА различных размерностей.

2. В каждом из типов используется скрытая коммутативная группа (обычно обладающая двухмерной цикличностью, но могут быть использованы скрытые группы с циклическим строением).

3. Секретный ключ включает в качестве своих элементов числа и векторы.

4. Открытый ключ включает в качестве своих элементов векторы.

5. Цифровая подпись включает в качестве своих элементов числа и вектор **S**.

6. Существенно используются операции возведения векторов в натуральную степень большого размера (от 80 до 256 бит и более).

Различие включает следующие существенные моменты:

1. Размерность КНАА, используемой в качестве алгебраического носителя, для алгоритмов первого типа выбирается исходя из требования наличия достаточно большого числа коммутативных групп и делимости порядка таких групп на простое число достаточно большого размера. Для алгоритмов второго типа наличие большого простого делителя порядка скрытой группы не является принципиальным требованием, а размерность КНАА играет существенную роль, так как является коэффициентом увеличения числа квадратных уравнений при сведении систем векторных квадратных уравнений к системам скалярных квадратных уравнений (квадратных уравнений в поле, над которым задана КНАА).

2. Строение ТУБВ, по которой задается операция умножения в КНАА, в алгоритмах первого типа не имеет непосредственного влияния на значение стойкости, а в алгоритмах второго типа — имеет, поскольку определяет число слагаемых в квадратных уравнениях, составляющих единую систему уравнений с многими неизвестными, вычислительная трудность решения которой определяет значение стойкости схемы ЭЦП.

3. Использование чисел в качестве элементов секретного ключа в схемах ЭЦП первого типа является принципиальным, поскольку они составляют значение дискретного логарифма в скрытой группе, а в схемах второго типа они играют вспо-

могательную роль в рамках приема повышения производительности процедуры генерации ЭЦП. При этом раскрытие этих численных значений не ведет к критическому снижению стойкости.

4. Включение вектора **S** в состав ЭЦП в алгоритмах ЭЦП первого типа имеет вспомогательное значение, а в алгоритмах второго типа — принципиальное. В первых ЭЦП может представлять собой пару или тройку чисел, а во вторых — единственный элемент в виде вектора **S**.

5. В алгоритмах первого типа операции экспоненцирования — это операции задания базовой вычислительно трудной задачи. В алгоритмах второго типа операции экспоненцирования используются как средство задания параметров и вычисления вектора **S**, удовлетворяющего проверочному уравнению с многократным вхождением **S**.

О выборе поля $GF(2^z)$ для задания КНАА как носителя схем ЭЦП второго типа

Элементы поля $GF(2^z)$, двоичные многочлены степени не более z, естественным образом записываются в виде z-битовых строк. При этом операция сложения представляет собой поразрядное сложение по модулю два, а умножение реализуется как многократное выполнение арифметических сдвигов битовых строк и указанных операций сложения. Для устранения операции арифметического деления операция умножения в $GF(2^z)$ задается по модулю неприводимого многочлена малого веса (трехчлена или пятичлена). Перечисленное обеспечивает достаточно быстрое выполнение операции умножения, а значит и операции экспоненцирования, в полях $GF(2^z)$ при программной и аппаратной реализации на различных технических платформах.

В алгебраических алгоритмах ЭЦП со скрытой группой, основанных на вычислительной трудности решения систем квадратных уравнений, выбор скрытой группы простого порядка не является наиболее предпочтительным случаем, поскольку факторизация ее порядка на делители малого размера не является критичной для обеспечения стойкости. Однако для повышения производительности процедуры генерации подписи используются приемы, включающие вычисление обратных значений по модулю, равному порядку скрытой группы. Это будет определять возникновение сравнительно частых случаев необходимости повтора вычислений (связанных с тем, что значения, от которых надо вычислить обратные, могут оказаться не взаимно простыми с модулем), если указанный порядок будет содержать простые делители малого размера.

Для практического устранения этого момента наиболее удобным является использование полей $GF(2^z)$, в которых число z является степенью Мерсенна, что задает простое значение числа $2^z - 1$ [20]. В интервале интересных для рассматриваемого применения значений z имеются следующие шесть чисел Мерсенна: 61, 89, 107, 127, 521 и 607. В промежутке от 127 до 521 степени Мерсенна отсутствуют. Однако, вполне приемлемо использовать также такие значения z, при которых число $2^z - 1$ содержит два или три больших простых делителя. В данном случае большим можно считать делитель размером 30 бит и более. Выполненные нами вычисления показали, что натуральные значения z такого типа имеются (см. табл. 2) и они встречаются чаще чисел Мерсенна, существенно расширяя возможности выбора различных сочетаний степени расширения поля $GF(2^z)$ и размерности КНАА.

Таблица 2

Значения степени расширения поля $GF(2^z)$, представляющие интерес при разработке алгоритмов ЭЦП второго типа

Степень z	Число простых делителей значения $2^z - 1$	Размер делителей, бит
61	1	61
89	1	89
101	2	43 и 59
103	2	39 и 63
107	1	107
109	2	30 и 80
127	1	127
137	2	65 и 73
139	2	43 и 97
149	2	67 и 83
173	3	41, 56 и 78
199	2	38 и 162

Пример алгебраической схемы ЭЦП второго типа

Воспользуемся в качестве алгебраического носителя четырехмерной КНАА, заданной над полем $GF(2^z)$ со степенью расширения $z = 149$. При этом операцию умножения четырехмерных векторов определим по табл. 1. В качестве структурных констант λ и μ возьмем единичные двоичные многочлены, т. е. $\lambda = \mu = 1$.

Для генерации секретного ключа воспользуемся следующей процедурой:

1. Сгенерировать базис <**G**, **H**> случайной коммутативной группы с двухмерной цикличностью, в котором каждый из векторов имеет порядок, равный значению $q = 2^{149} - 1 =$ $= 713623846352979940529142984724747568191373311$.

2. Сгенерировать случайные попарно неперестановочные обратимые векторы **A**, **B**, и **D**, каждый из которых также неперестановочен с вектором **G**.

3. Сгенерировать случайные натуральные числа x, w и u ($1 < x, w, u < q$).

4. Вычислить четырехмерные векторы $\mathbf{G}_x = \mathbf{G}^x$, $\mathbf{G}_u = \mathbf{G}^u$ и $\mathbf{H}_w = \mathbf{H}^w$ (векторы **G**, **H**, $\mathbf{G}_x$, $\mathbf{G}_u$ и $\mathbf{H}_w$ являются попарно перестановочными как принадлежащие коммутативной группе, генерируемой базисом <**G**, **H**>).

На выходе процедуры генерации секретного ключа получаем его значение в виде набора векторов **A**, **B**, **D**, **G**, **H**, $\mathbf{G}_x$, $\mathbf{G}_u$ и $\mathbf{H}_w$ и чисел x, w и u, имеющего общий размер ≈652 байт (на самом деле векторы $\mathbf{G}_x$, $\mathbf{G}_u$ и $\mathbf{H}_w$ можно не включать в состав секретного ключа, поскольку их можно вычислить по формулам из п. 4 описанной процедуры; в этом случае имеем размер секретного ключа, равный ≈429 байт).

Процедура формирования открытого ключа в виде набора четырехмерных векторов $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$ и **P**, зависящих от секретного ключа, состоит в выполнении вычислений по следующим формулам:

$$\mathbf{Y}_1 = \mathbf{AGB},\ \mathbf{Z}_1 = \mathbf{DHA}^{-1}, \tag{1}$$

$$\mathbf{Y}_2 = \mathbf{AH}_w\mathbf{B},\ \mathbf{Z}_2 = \mathbf{DG}_x\mathbf{A}^{-1} \text{ и } \mathbf{P} = \mathbf{AG}_u\mathbf{HA}^{-1}. \tag{2}$$

Заметим, что вместо (2) могут быть использованы формулы с операцией возведения в степень:

$$\mathbf{Y}_2 = \mathbf{AH}^w\mathbf{B},\ \mathbf{Z}_2 = \mathbf{DG}^x\mathbf{A}^{-1} \text{ и } \mathbf{P} = \mathbf{AG}^u\mathbf{HA}^{-1}. \tag{3}$$

Применение формул (3) относится к случаю, когда векторы $\mathbf{G}_x$, $\mathbf{G}_u$ и $\mathbf{H}_w$ выведены из состава секретного ключа. Длина (размер) открытого ключа равна ≈373 байт.

Процедура генерации ЭЦП.

1. Используя некоторую специфицированную 384-битную хэш-функцию f_H, вычисляют хэш-значение $h = h_1\|h_2\|h_3 = f_H(M)$ от подписываемого электронного документа M (знак || обозначает операцию конкатенации).

2. Вычислить целочисленные значения n и d по следующим двум формулам:

$$n = \frac{xh_2 + uh_3 - h_1}{h_1 - h_2} \bmod q \text{ и} \tag{4}$$

$$d = \frac{wh_2 + h_3 - h_1}{h_1 - h_2} \bmod q. \tag{5}$$

3. Вычислить ЭЦП в виде четырехмерного вектора **S** по формуле

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^n\mathbf{H}^d\mathbf{D}^{-1}. \tag{6}$$

Вычислительная трудоемкость процедуры генерации ЭЦП можно приближенно оценить как две операции экспоненцирования четырехмерных векторов, которые пересчитываются в ≈3576 операций умножения в поле $GF(2^{149})$. Размер подписи равен ≈75 байт.

Процедура верификации ЭЦП.

1. Вычисляют 384-битное хэш-значение $h = h_1\|h_2\|h_3 = f_H(M)$ от подписанного документа, которое представлено в виде конкатенации трех 128-битных чисел h_1, h_2 и h_3.

2. Проверить выполнимость проверочного уравнения

$$\left(\mathbf{Y}_1\mathbf{SZ}_1\right)^{h_1} = \left(\mathbf{Y}_2\mathbf{SZ}_2\right)^{h_2}\mathbf{P}^{h_3}. \tag{7}$$

3. Если равенство (7) выполняется, то ЭЦП к документу M признается подлинной, в противном случае ЭЦП отвергается.

Вычислительная трудоемкость процедуры верификации ЭЦП примерно равна трем операциям экспоненцирования четырехмерных векторов, которые пересчитываются в ≈5364 операций умножения в $GF(2^{149})$.

Легко видеть, что вычисление секретного ключа по открытому ключу связано с решением системы из 9 квадратных векторных уравнений с 8 неизвестными **A**, **B**, **D**, **G**, **H**, $\mathbf{G}_x$, $\mathbf{G}_u$ и $\mathbf{H}_w$, заданной над использованной четырехмерной КНАА. Вид векторных уравнений задается формулами (1) и (2), дополненными условиями перестановочности вектора **G** с векторами **H**, $\mathbf{G}_x$, $\mathbf{G}_u$ и $\mathbf{H}_w$. Указанная система векторных уравнений (совместная по построению) сводится к системе из 36 уравнений с 32 неизвестными, заданной над полем $GF(2^z)$ со 149-битным порядком.

Корректность описанной схемы ЭЦП легко доказывается путем демонстрации того, что корректно вычисленная ЭЦП в соответствии с процедурой генерации ЭЦП проходит процедуру верификации ЭЦП. Действительно пусть четырехмерный вектор **S** представляет собой корректно вычисленную ЭЦП. Тогда имеем такое доказательство корректности предложенной схемы ЭЦП (вычисляем последовательно левую и правую части проверочного уравнения (7)):

$$\mathbf{K}_L = \left(\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1\right)^{h_1} = \left(\mathbf{AGBB}^{-1}\mathbf{G}^n\mathbf{H}^d\mathbf{D}^{-1}\mathbf{DHA}^{-1}\right)^{h_1} = \left(\mathbf{AG}^{n+1}\mathbf{H}^{d+1}\mathbf{A}^{-1}\right)^{h_1} = \mathbf{AG}^{nh_1+h_1}\mathbf{H}^{dh_1+h_1}\mathbf{A}^{-1} =$$

$$= \mathbf{AG}^{\frac{xh_2+uh_3-h_1}{h_1-h_2}h_1+h_1}\mathbf{H}^{\frac{wh_2+h_3-h_1}{h_1-h_2}h_1+h_1}\mathbf{A}^{-1} = \mathbf{AG}^{\frac{xh_1h_2+uh_1h_3-h_1h_2}{h_1-h_2}}\mathbf{H}^{\frac{wh_1h_2+h_1h_3-h_1h_2}{h_1-h_2}}\mathbf{A}^{-1};$$

$$\mathbf{K}_R = \left(\mathbf{Y}_2\mathbf{S}\mathbf{Z}_2\right)^{h_2}\mathbf{P}^{h_3} = \left(\mathbf{AH}^w\mathbf{BB}^{-1}\mathbf{G}^n\mathbf{H}^d\mathbf{D}^{-1}\mathbf{DG}^x\mathbf{A}^{-1}\right)^{h_2}\mathbf{P}^{h_3} = \left(\mathbf{AG}^{n+x}\mathbf{H}^{w+d}\mathbf{A}^{-1}\right)^{h_2}\left(\mathbf{AG}^u\mathbf{HA}^{-1}\right)^{h_3} =$$

$$= \mathbf{AG}^{nh_2+xh_2}\mathbf{H}^{wh_2+dh_2}\mathbf{A}^{-1}\mathbf{AG}^{uh_3}\mathbf{H}^{h_3}\mathbf{A}^{-1} = \mathbf{AG}^{nh_2+xh_2+uh_3}\mathbf{H}^{dh_2+wh_2+h_3}\mathbf{A}^{-1} =$$

$$= \mathbf{AG}^{\frac{xh_2+uh_3-h_1}{h_1-h_2}h_2+xh_2+uh_3}\mathbf{H}^{\frac{wh_2+h_3-h_1}{h_1-h_2}h_2+wh_2+h_3}\mathbf{A}^{-1} = \mathbf{AG}^{\frac{xh_1h_2+uh_1h_3-h_1h_2}{h_1-h_2}}\mathbf{H}^{\frac{wh_1h_2+h_1h_3-h_1h_2}{h_1-h_2}}\mathbf{A}^{-1} = \mathbf{K}_L.$$

Поскольку проверочное уравнение (7) выполняется, то правильно сгенерированная ЭЦП проходит процедуру верификации как подлинная подпись, т. е. предложенная схема ЭЦП со скрытой группой работает корректно.

Сравнение с известными алгоритмами многомерной криптографии

Известные двухключевые криптосхемы (алгоритмы ЭЦП, алгоритмы открытого распределения ключей и открытого шифрования), основанные на вычислительной трудности решения систем многих квадратных уравнений с многими неизвестными относятся к многомерной криптографии [7,8]. С этими криптосхемами предложенный алгоритм имеет общность по базовой вычислительно трудной задаче, лежащей в основе их стойкости. В остальном он совершенно не похож на алгоритмы многомерной криптографии. Можно отметить следующие важные различия:

1. В криптосхемах многомерной криптографии разработчик алгоритма вырабатывает функции от многих переменных, которые определяют вид квадратных уравнений, образующих единую систему уравнений. В предложенном алгоритме система квадратных уравнений вытекает из уравнений, задающих связь секретного ключа с открытым, которые составляются как часть разрабатываемой процедуры генерации открытого ключа в зависимости от секретного ключа.

2. В двухключевых криптосхемах многомерной криптографии разрабатываются функции от многих переменных над полями $GF(2^z)$ сравнительно малого порядка, равного значениям от 2^4 до 2^{16}. Соответственно возникают системы многих квадратных уравнений над такими полями. В предложенном алгебраическом алгоритме со скрытой группой возникающая система квадратных уравнений задана над полями достаточно большого порядка, равного 2^{149}.

3. В криптосхемах многомерной криптографии число квадратных уравнений, входящих в единую систему может быть больше, равно или меньше числа неизвестных. В предложенном алгоритме ЭЦП число уравнений в системе квадратных уравнений может быть равно или больше числа неизвестных.

4. Размер ЭЦП в обеих сравниваемых схемах ЭЦП является достаточно малым, а размер открытого ключа в схемах ЭЦП многомерной криптографии в сотни раз превышает размер открытого ключа в предложенном алгебраическом алгоритме со скрытой группой.

Отвлекаясь от конкретного вида квадратных уравнений входящих в единую систему, трудность решения которой определяет уровень стойкости криптосхемы, для оценки последнего можно предложить общий неформальный показатель ψ, равный произведению числа неизвестных η на двоичный логарифм порядка поля над которым задаются квадратные уравнения. На основе сравнения значения показателя ψ для различных алгоритмов ЭЦП можно сделать некоторые предварительные сравнительные оценки стойкости по критерию "более высокие значения ψ соответствуют более высокой стойкости". Однако окончательные оценки о значении стойкости могут быть сделаны только на основе детального рассмотрения вычислительной сложности каждой конкретной системы квадратных уравнений.

Сопоставление нескольких известных алгоритмов ЭЦП многомерной криптографии и предложенного алгебраического алгоритма ЭЦП приведено в табл. 3. Сравнение показывает ряд существенных преимуществ алгоритмов ЭЦП со скрытой группой.

Таблица 3

Сравнение с известными алгоритмами ЭЦП многомерной криптографии

Алгоритм ЭЦП	Размер ЭЦП, байт	Размер открытого ключа, байт	Число квадратных уравнений (неизвестных)	Порядок поля, над которым заданы уравнения	Показатель Ψ
[7]	—	—	27 (27)	2^{16}	432
Rainbow [21]	33	16065	27 (33)	2^8	264
QUARTZ [8]	16	72704	100 (107)	2^4	428
Rainbow [22] (3 разных версии)	66… 204	>150000 … >1900000	64 (96)… 128 (204)	2^4, 31, 2^8	384… 1632
[6]	160	512	28 (28)	$>2^{256}$	>7168
предложенный	75	373	36 (32)	2^{149}	4768

Заключение

Использование КНАА, заданных над конечными полями характеристики два в качестве алгебраического носителя алгоритмов ЭЦП со скрытой группой, основанных на вычислительной трудности решения систем многих квадратичных уравнений с многими неизвестными, позволяет построить практичные постквантовые схемы ЭЦП. Примером является предложенная новая схема ЭЦП со срытой группой, реализованная на четырехмерной КНАА, заданной по прореженной ТУБВ над полем $GF(2^{149})$. Представляют интерес аналогичные реализации с использованием шестимерных КНАА, однако для этого требуется изучить строение последних или, по крайней мере, установить строение коммутативных групп, содержащихся в указанных алгебрах.

Работа выполнена при финансовой поддержке РФФИ (проект № 21-57-54001-Вьет_а).

Литература

1. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM Journal of Computing. 1997. V. 26. P. 1484—1509.
2. *Smolin J. A., Smith G., Vargo A.* Oversimplifying quantum factoring // Nature. 2013. V. 499. № 7457. P. 163—165.
3. *Молдовян А. А., Молдовян Д. Н.* Постквантовая схема ЭЦП на основе скрытой задачи дискретного логарифмирования в четырехмерной конечной алгебре // Вопросы защиты информации. 2019. № 2. С. 18—22.
4. *Moldovyan N. A., Moldovyan A. A.* Candidate for practical post-quantum signature scheme // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2020. Т. 16. Вып. 4. С. 455—461. DOI: 10.21638/11701/spbu10.2020.410.
5. *Молдовян А. А., Молдовян Н. А., Молдовян Д. Н., Костина А. А.* Новый подход к разработке алгоритмов цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2021. № 4. С. 45—49. DOI: 10.52190/2073-2600_2021_4_45.
6. *Молдовян Д. Н., Молдовян А. А., Молдовян Н. А.* Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах // Вопросы кибербезопасности. 2022. № 1(47). С. 18—25. DOI: 10.21681/2311-3456-2022-1-18-25.
7. *Shuaiting Q., Wenbao H., Yifa Li, Luyao J.* Construction of Extended Multivariate Public Key Cryptosystems // International Journal of Network Security. 2016. V. 18. № 1. P. 60—67.
8. *Jintai D., Dieter S.* Multivariable Public Key Cryptosystems (2004) [Электронный ресурс]. Режим доступа: https://eprint.iacr.org/2004/350.pdf (дата обращения: 21 января 2022 г.).
9. *Молдовян Д. Н.* Задание шестимерных алгебр как носителей криптосхем, основанных на скрытой задаче дискретного логарифмирования // Вопросы защиты информации. 2021. № 1. С. 26—32. DOI: 10.52190/2073-2600_2021_1_26.
10. *Moldovyan N. A.* Fast Signatures Based on Non-Cyclic Finite Groups // Quasigroups and Related Systems. 2010. V. 18. № 1. P. 83—94.
11. *Moldovyan N. A., Moldovyan A. A.* Finite Non-commutative Associative Algebras as Carriers of Hidden Discrete Logarithm Problem // Вестник ЮУрГУ. Серия "Математическое моделирование и программирование". 2019. Т. 12. № 1. С. 66—81. DOI: 10.14529/mmp190106.
12. *Moldovyan N. A., Moldovyan A. A.* Candidate for practical post-quantum signature scheme // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2020. Т. 16. Вып. 4. С. 455—461. DOI: 10.21638/11701/spbu10.2020.410.
13. *Молдовян Н. А., Абросимов И. К.* Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23—32.
14. *Moldovyan N. A.* Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. № 2(93). P. 62—67.
15. *Moldovyan N. A.* Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions // Quasigroups and Related Systems. 2018. V. 26. № 2. P. 263—270.
16. *Moldovyan D. N.* A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. V. 29. № 2(86). P. 206—226.
17. *Молдовян Д. Н., Молдовян А. А., Костина А. А.* Постквантовая схема цифровой подписи с двойным маскированием операции экспоненциирования // Вопросы защиты информации. 2020. № 2. С. 41—48.
18. *Moldovyan N. A., Moldovyanu P. A.* New primitives for digital signature algorithms // Quasigroups and Related Systems. 2009. V. 17. № 2. P. 271—282.

19. *Moldovyan N. A.* Fast signatures Based on Non-cyclic finite groups // Quasigroups and Related Systems. 2010. V. 18. № 1. P. 83—94.

20. *Crandall R., Pomerance C.* Prime Numbers — A Computational Perspective. — New York: Springer, 2002.

21. *Ding J., Schmidt D.* Rainbow, a new multivariable polynomial signature scheme: in Conference on Applied Cryptography and Network Security — ACNS 2005. Springer Lecture Notes in Computer Science. 2005. V. 3531. P. 164—175.

22. Rainbow Signature. One of three NIST Post-quantum Signature Finalists [on line] 2021. [Электронный ресурс]. Режим доступа: https://www.pqcrainbow.org/ (дата обращения: 21 января 2022 г.).

Algebraic algorithms with a hidden group over finite fields with binary characteristic

A. A. Kurysheva, A. A. Kostina, N. A. Moldovyan
St. Petersburg Federal Research Center of the RAS (SPC RAS), St. Petersburg, Russia

The features of the implementation of digital signature algorithms on finite noncommutative associative algebras set over the finite fields of binary characteristics are considered. Interest in the implementation of such type is associated with the possibility of improving the productivity of algorithms with a hidden group, as well as with the fact that the security of the algorithms is based on the computational difficulty of solving systems of quadratic equations. The factorization of the order of the hidden group is non-critical for the security of the signature algorithm, so it is possible to use the GF(2^z) fields not only with the values of the degree that equals to a Mersenne exponent, but also with other z values. As an algebraic carrier of algorithms, the algebras specified on the sparse basis vector multiplication tables are considered. The main types of commutative groups contained in such algebras are established, which represent interest for using them as a hidden group.

Keywords: information security, digital signature, post-quantum cryptography, finite associative algebra, noncommutative algebra, hidden group.

Bibliography — 22 references. *Received January 29, 2022*

УДК 003.26
DOI: 10.52190/2073-2600_2022_2_21
EDN: JQWUAP

Конечные кватернионоподобные алгебры как носители постквантовых алгоритмов ЭЦП

А. А. Молдовян, д-р техн. наук; *Д. Н. Молдовян*, канд. техн. наук
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Санкт-Петербург, Россия

Н. А. Молдовян, д-р техн. наук; *А. А. Костина*
Санкт-Петербургский федеральный исследовательский центр РАН (СПб ФИЦ РАН),
Санкт-Петербург, Россия

Рассмотрена декомпозиция конечных четырехмерных ассоциативных алгебр, некоммутативность операции умножения в которых задана несимметричным распределением структурной константы, на коммутативные подалгебры. Установлены типы подалгебр и значения порядков их мультипликативных групп. Полученные результаты показывают возможность применения изученных четырех конечных кватернионоподобных алгебр в качестве носителей постквантовых алгоритмов цифровой подписи со скрытой группой, в том числе, основанных на вычислительной трудности нахождения решения системы многих квадратных уравнений с многими неизвестными.

Ключевые слова: информационная безопасность, постквантовая криптография, цифровая подпись, конечная ассоциативная алгебра, некоммутативная алгебра, циклическая группа, двухмерная цикличность.

Объявленная Национальным институтом стандартов и технологий США (НИСТ) программа на 2017—2024 гг. по разработке стандартов на постквантовые двухключевые криптоалгоритмы [1] является свидетельством об актуальности исследований в области постквантовой криптографии. Проводимый в настоящее время конкурс по разработке алгоритмов указанного типа [2, 3] выявил определенные проблемы по созданию практичных постквантовых алгоритмов электронной цифровой подписи (ЭЦП), которые побудили НИСТ принять предварительное решение об анонсировании принятия новых заявок в номинации постквантовых ЭЦП [4]. Основными недостатками отобранных финалистов в номинации алгоритмов ЭЦП является достаточно большой размер подписи и/или открытого ключа. Для устранения этого недостатка, видимо, при разработке следует использовать новые подходы. В качестве перспективного подхода можно рассматривать способ [5—7] построения постквантовых алгебраических алгоритмов ЭЦП со скрытой группой, стойкость которых основана на вычислительной трудности нахождения решения системы многих квадратных уравнений с многими неизвестными. В этом способе в качестве секретного элемента используется коммутативная группа достаточно большого порядка, содержащаяся в конечной некоммутативной ассоциативной алгебре (КНАА), которая включает достаточно большое число коммутативных групп одного порядка. Этот момент делает актуальным изучение строения КНАА как алгебраических носителей алгоритмов ЭЦП со скрытой группой, а именно рассмотрение вопроса декомпозиции КНАА на коммутативные подалгебры. Для КНАА, заданных по прореженным таблицам умножения базисных векторов (ТУБВ), данная задача решена в работах [8—10]. Кватернионоподобные алгебры, предложенные в [11, 12], представляют значительный интерес в качестве алгебраических носителей алгоритмов ЭЦП со скрытой группой, основанных на вычислительной трудности решения систем квадратных уравнений. Последнее определяет актуальность исследования строения кватернионоподобных КНАА.

В данной работе исследован вопрос о декомпозиции четырех типов кватернионоподобных КНАА на коммутативные подалгебры и показана

Молдовян Александр Андреевич, профессор.
E-mail: maa1305@yandex.ru
Молдовян Дмитрий Николаевич, доцент.
E-mail: mdn.spectr@mail.ru
Молдовян Николай Андреевич, профессор, главный научный сотрудник.
E-mail: nmold@mail.ru
Костина Анна Александровна, научный сотрудник.
E-mail: anya@hotbox.ru

Статья поступила в редакцию 6 мая 2022 г.

общность строения указанных алгебр и потенциальная возможность их использования в качестве алгебраических носителей постквантовых схем ЭЦП со скрытой группой.

Кватернионоподобные алгебры

Конечные алгебры задаются как конечное m-мерное векторное пространство над конечным полем, в котором дополнительно определена замкнутая операция умножения всевозможных пар векторов, обладающая свойствами дистрибутивности слева и справа относительно операции сложения. Некоторый вектор **A** можно записать в виде 1) упорядоченного набора координат: $\mathbf{A} = (a_0, a_1, \ldots, a_{m-1})$ и 2) в виде суммы однокомпонентных векторов $a_i\mathbf{e}_i$: $\mathbf{A} = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$, где $\mathbf{e}_i$ — базисные векторы; a_i — элементы конечного поля, над которым задано векторное пространство. С учетом того, что будут рассматриваться кватернионоподобные конечные алгебры, в качестве конечного поля используется простое поле $GF(p)$ с нечетным значением характеристики p.

Свойство двухсторонней дистрибутивности и замкнутости операции умножения векторов $\mathbf{A} = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$ и $\mathbf{B} = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ обеспечивается ее определением как перемножение каждой компоненты вектора **A** с каждой компонентой вектора **B**, выполняемое в соответствии со следующей формулой:

$$\mathbf{A} \circ \mathbf{B} = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \left(\mathbf{e}_i \circ \mathbf{e}_j\right), \qquad (1)$$

в которой всевозможные произведения пар базисных векторов $\mathbf{e}_i \circ \mathbf{e}_j$ заменяются на соответствующие однокомпонентные векторы, задаваемые некоторой ТУБВ, например, представленной в виде табл. 1. А именно, каждое из произведений $\mathbf{e}_i \circ \mathbf{e}_j$ заменяется на некоторый вектор $\lambda\mathbf{e}_k$, указанный в ячейке на пересечении i-й строки и j-го столбца. Значение $\lambda \neq 1$ называется структурной константой.

Таблица 1

Таблица, задающая умножение в конечной алгебре кватернионов с глобальной двухсторонней единицей вида E = (1, 0, 0, 0)

•	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\mathbf{e}_1$	$-\mathbf{e}_0$	$\mathbf{e}_3$	$-\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_2$	$-\mathbf{e}_3$	$-\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\mathbf{e}_2$	$-\mathbf{e}_1$	$-\mathbf{e}_0$

Конечная алгебра кватернионов характеризуется следующим набором свойств ТУБВ:

- симметричность распределения базисных векторов относительно главной диагонали, проходящей из верхнего левого угла в правый нижний;
- несимметричность распределения по ячейкам структурного коэффициента $\lambda = -1$, за счет чего обеспечивается некоммутативность операции умножения;
- задание ассоциативного умножения.

Четырехмерные КНАА, заданные по ТУБВ с указанным набором свойств будем называть кватернионоподобными алгебрами, примеры которых представлены в работах [11, 12]. Достаточно очевидно, что кватернионоподобные КНАА задаются над конечными полями нечетной характеристики, поскольку в полях четной характеристики, значения 1 и –1 совпадают.

Известные примеры [11, 12] кватернионоподобных алгебр могут быть обобщены путем включения в ТУБВ нескольких независимых структурных констант со значением –1 и нескольких независимых структурных констант с произвольными значениями, отличными от нуля. В результате такого обобщения получены следующие четыре типа кватернионоподобных КНАА, задаваемых по табл. 2—5, в которых независимые структурные константы k, q, p, s, t и u равны –1 или 1 и каждая из них распределена несимметрично относительно главной диагонали, причем каждая из них присутствует в четырех ячейках таблицы. Комбинация значений констант k, q, p, s, t и u выбирается такой, что результирующее значение –1 присутствует в несимметрично распределенных ячейках ТУБВ, что определяет свойство некоммутативности операции умножения. Структурные константы α, β и λ, распределенные симметрично относительно главной диагонали, принимают произвольные значения, отличные от нуля. Если одна или более из констант α, β и λ равна нулю, то имеем вырожденный случай.

В алгебре кватернионов базисные векторы $\mathbf{e}_0$, $\mathbf{e}_1$, $\mathbf{e}_2$ и $\mathbf{e}_3$ обычно обозначаются как **e**, **i**, **j** и **k** соответственно. Кватернионоподобные КНАА будем называть в соответствии с базисным вектором **e**, **i**, **j** или **k**, содержащимся во всех клетках на главной диагонали, что отражено в названиях табл. 2—5.

Таблица 2

Задание конечных алгебр e-кватернионов с единицей E = (1, 0, 0, 0).

•	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\mathbf{e}_1$	$qu\alpha\lambda\ \mathbf{e}_0$	$kqs\alpha\mathbf{e}_3$	$ksu\lambda\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_2$	$ptu\alpha\mathbf{e}_3$	$ps\alpha\beta\mathbf{e}_0$	$stu\beta\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$qpt\lambda\mathbf{e}_2$	$kqp\beta\mathbf{e}_1$	$kt\lambda\beta\mathbf{e}_0$

Устанавливая различные комбинации значений структурных констант k, q, p, s, t, u, α, β и λ из области их допустимых значений, можно получить большое число различных КНАА для каждого из следующих четырех типов: **e**-, **i**-, **j**- и **k**-кватернионов.

Алгебра **e**-кватернионов впервые упоминается в работе [11] как частный случай построения КНАА с использованием унифицированного способа задания ассоциативных алгебр произвольных четных размерностей. Упомянутый способ реализует некоммутативные алгебры для размерностей $m \geq 6$ и коммутативные для случаев $m = 2$ и $m = 4$. При этом для последнего случай в работе [11] отмечается, что некоммутативность операции умножения может быть достигнута внесением несимметрично распределенной структурой константы –1, и приведены несколько вариантов реализации четырехмерных КНАА, один из которых соответствует алгебре кватернионов. Таблица 2 задает расширенные варианты реализации **e**-кватернионов.

Частные случаи алгебр **i**-, **j**- и **k**-кватернионов предложены в статье [12], в которой они рассматриваются в качестве алгебраического носителя алгоритмов ЭЦП со скрытой группой, основанных на скрытой задаче дискретного логарифмирования. Найденные авторами расширенные варианты этих трех типов кватернионоподобных КНАА представлены табл. 3—5. Распределения базисных векторов, имеющее место в алгебрах **j**- и **k**-кватернионов, встречались также в конечных коммутативных ассоциативных алгебрах, использованных в качестве единого алгебраического носителя в схеме ЭЦП с удвоенным проверочным уравнением [13].

Таблица 3

Задание конечных алгебр i-кватернионов с единицей E = (0, 1, 0, 0)

•	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$pu\alpha\lambda\mathbf{e}_1$	$\mathbf{e}_0$	$kpt\lambda\mathbf{e}_3$	$ktu\alpha\mathbf{e}_2$
$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_2$	$qsu\lambda\mathbf{e}_3$	$\mathbf{e}_2$	$kq\beta\lambda\mathbf{e}_1$	$ksu\beta\mathbf{e}_0$
$\mathbf{e}_3$	$qps\alpha\mathbf{e}_2$	$\mathbf{e}_3$	$qpt\beta\mathbf{e}_0$	$st\alpha\beta\mathbf{e}_1$

Таблица 4

Задание конечных алгебр j-кватернионов с единицей E = (0, 0, 1, 0)

•	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$kp\alpha\lambda\mathbf{e}_2$	$ktu\alpha\mathbf{e}_3$	$\mathbf{e}_0$	$ptu\lambda\mathbf{e}_1$
$\mathbf{e}_1$	$qps\alpha\mathbf{e}_3$	$qt\alpha\beta\mathbf{e}_2$	$\mathbf{e}_1$	$pst\beta\mathbf{e}_0$
$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$kqs\lambda\mathbf{e}_1$	$kqu\beta\mathbf{e}_0$	$\mathbf{e}_3$	$su\beta\lambda\mathbf{e}_2$

Таблица 5

Задание конечных алгебр k-кватернионов с единицей E = (0, 0, 0, 1)

•	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$kp\beta\lambda\mathbf{e}_3$	$kts\beta\mathbf{e}_2$	$pts\lambda\mathbf{e}_1$	$\mathbf{e}_0$
$\mathbf{e}_1$	$pqu\beta\mathbf{e}_2$	$qs\alpha\beta\mathbf{e}_3$	$psu\alpha\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_2$	$kqu\lambda\mathbf{e}_1$	$kqt\alpha\mathbf{e}_0$	$ut\alpha\lambda\mathbf{e}_3$	$\mathbf{e}_2$
$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$

Общие свойства исследованных алгебр

Достаточно легко показать, что в каждой из исследованных алгебр векторные уравнения $\mathbf{XA} = \mathbf{A}$ и $\mathbf{AX} = \mathbf{A}$ относительно неизвестного вектора $\mathbf{X}$ имеют одно и то же единственное решение, которое представляет собой глобальную двухстороннюю единицу $\mathbf{E}$. При этом значения $\mathbf{E}$ различны в кватернионоподобных алгебрах различных типов. Значения глобальной двухсторонней единицы указаны в названиях табл. 2—5.

Также легко показать, что во всех кватернионоподобных алгебрах векторные уравнения $\mathbf{XA} = \mathbf{E}$ и $\mathbf{AX} = \mathbf{E}$ либо одновременно не имеют решений, либо имеют одно и то же единственное решение $\mathbf{X} = \mathbf{A}^{-1}$, которое называется обратным значением вектора $\mathbf{A}$. В первом случае вектор $\mathbf{A}$ называется необратимым вектором, а во втором — обратимым. Очевидно векторы $\mathbf{A}$ и $\mathbf{A}^{-1}$ являются перестановочными.

Векторы вида $\mathbf{L} = \lambda\mathbf{E}$, где λ — скалярный множитель ($\lambda \in GF(p)$), называются скалярными векторами. Легко показать, что каждый фиксированный скалярный вектор перестановочен со всеми четырехмерными векторами, содержащимися в каждой фиксированной кватернионоподобной алгебре.

Строение кватернионоподобных алгебр k-типа

Рассмотрение нескольких произвольно выбранных частных случаев алгебр **k**-кватернионов показало, что единичным вектором в них является вектор $\mathbf{E} = (0,0,0,1)$, причем эта единица является глобальной двухсторонней единицей (т. е. действует как единица слева и справа на каждый четырехмерный вектор). Все изученные частные случаи алгебр **k**-кватернионов имеют сходное строение в смысле декомпозиции на коммутативные подалгебры. Рассмотрим метод изучения декомпозиции на примере исследования частного случая, заданного табл. 6.

Таблица 6

Изученный случай алгебр k-кватернионов

•	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\lambda\mathbf{e}_3$	$\mathbf{e}_2$	$\lambda\mathbf{e}_1$	$\mathbf{e}_0$
$\mathbf{e}_1$	$-\mathbf{e}_2$	$\mathbf{e}_3$	$-\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_2$	$-\lambda\mathbf{e}_1$	$\mathbf{e}_0$	$-\lambda\mathbf{e}_3$	$\mathbf{e}_2$
$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$

Пусть задан некоторый вектор $\mathbf{A} = (a_0, a_1, a_2, a_3)$. Найдем множество векторов, перестановочных с **A**. Для этого найдем все решения следующего векторного уравнения с неизвестным значением $\mathbf{X} = (x_0, x_1, x_2, x_3)$:

$$\mathbf{XA} = \mathbf{AX}. \tag{2}$$

Используя формулу (1) и табл. 6, можно легко свести решение уравнения (2) к решению системы из трех скалярных линейных уравнений следующего вида:

$$\begin{cases} a_1 x_2 = a_2 x_1; \\ a_2 x_0 = a_0 x_2; \\ a_1 x_0 = a_0 x_1. \end{cases} \tag{3}$$

Координата x_3 не входит в систему (3), поэтому пространство решений, которое зависит от значения вектора **A**, включает векторы со всевозможными значениями $x_3 = 1, 2, \ldots, p-1$. Следует рассмотреть следующие случаи:

1. Вектор **A** является скалярным, т. е. $a_0 = a_1 = a_2 = 0$. Очевидно, что множество $\Psi_\mathbf{A}$ векторов, перестановочных с **A**, совпадает с рассматриваемой некоммутативной алгеброй.

2. Случай $a_1 \neq 0$. Тогда, с учетом соотношений $x_2 = a_2 a_1^{-1} x_1$ и $x_0 = a_0 a_1^{-1} x_1$, система (3) сводится к следующей системе из двух линейных уравнений:

$$\begin{cases} x_2 = \dfrac{a_2}{a_1} x_1; \\ x_0 = \dfrac{a_0}{a_1} x_1, \end{cases} \tag{4}$$

которые непосредственно описывают значения неизвестных координат x_0 и x_2, при которых значение вектора является решением векторного уравнений (2), для всевозможных пар значений координат x_1, $x_3 = 1, 2, \ldots, p-1$. Таким образом, при $a_1 \neq 0$ $\Psi_\mathbf{A}$ описывается следующей формулой

$$\mathbf{X} = (x_0, x_1, x_2, x_3) = \left(\frac{a_0}{a_1} j,\ j,\ \frac{a_2}{a_1} j,\ k \right), \tag{5}$$

где $j, k = 0, 1, 2, \ldots, p-1$. При $j = 0$ множество (5) описывает всевозможные скалярные векторы.

Утверждение 1. Пусть дан вектор $\mathbf{B} = (b_0, b_1, b_2, b_3) \in \Psi_\mathbf{A}$, такой, что $b_1 \neq 0$. Тогда множество $\Psi_\mathbf{B}$ векторов, перестановочных с **B**, совпадает с $\Psi_\mathbf{A}$.

Доказательство. Учитывая, что $b_1 \neq 0$, поэтому $\Psi_\mathbf{B}$ описывается формулой (5) при $j' = 1, 2, \ldots, p-1$ и $k' = 0, 1, 2, \ldots, p-1$, причем $\mathbf{B} = \left(a_0 a_1^{-1} j',\ j',\ a_2 a_1^{-1} j',\ k' \right)$, имеем следующую формулу для описания всех векторов $\mathbf{X}' \in \Psi_\mathbf{B}$:

$$\begin{aligned} \mathbf{X}' = (x_0', x_1', x_2', x_3') &= \left(\frac{b_0}{b_1} j,\ j,\ \frac{b_2}{b_1} j,\ k \right) = \\ &= \left(\frac{a_0 a_1^{-1} j'}{j'} j,\ j,\ \frac{a_0 a_1^{-1} j'}{j'} j,\ k \right) = \\ &= \left(\frac{a_0}{a_1} j,\ j,\ \frac{a_2}{a_1} j,\ k \right). \end{aligned}$$

Таким образом, множества $\Psi_\mathbf{B}$ и $\Psi_\mathbf{A}$ содержат одни и те же векторы, что требовалось доказать. (Заметим, что множество (5) включает векторы с фиксированными отношениями x_0/x_1 и x_2/x_1.)

Утверждение 2. Пусть даны векторы **B** и **D**, перестановочные с вектором **A**. Тогда векторы **B** и **D** перестановочны, т. е. **BD** = **DB**.

Доказательство. В соответствии с утверждением 1 имеем $\Psi_\mathbf{B} = \Psi_\mathbf{A}$, поэтому $\mathbf{D} \in \Psi_\mathbf{B}$, т. е. вектор **D** перестановочен с **B**.

Утверждение 3. Множество векторов $\Psi_\mathbf{A}$ образует коммутативную подалгебру порядка p^2.

Доказательство. Очевидно, что нулевой вектор $\mathbf{O} = (0, 0, 0, 0)$ и глобальная двухсторонняя единица **E** содержатся в $\Psi_\mathbf{A}$. Пусть дан некоторый обратимый вектор $\mathbf{B} \in \Psi_\mathbf{A}$. Тогда в силу перестановочности векторов **B** и $\mathbf{B}^{-1}$ (см. предыдущий раздел) имеем $\mathbf{B}^{-1} \in \Psi_\mathbf{A}$, т. е. векторы обратимые в рассматриваемой КНАА также обратимы в рамках $\Psi_\mathbf{A}$. Теперь покажем, что произведение произвольных двух векторов $\mathbf{B} \in \Psi_\mathbf{A}$ и $\mathbf{D} \in \Psi_\mathbf{A}$ также содержится в $\Psi_\mathbf{A}$: **A**(**BD**) = **BAD** = **BDA** = (**BD**)**A**. Остальные свойства операций сложения и умножения рассматриваемой некоммутативной алгебры также легко переносятся на $\Psi_\mathbf{A}$, т. е. $\Psi_\mathbf{A}$ является коммутативной подалгеброй.

3. Случай $a_1 = 0$. Тогда любая пара значений $x_2 \in GF(p)$ и $x_0 \in GF(p)$ удовлетворяет первому и третьему уравнениям системы (3) при $x_1 = 0$. При этом, если $a_0 = 0$ и $a_2 = 0$, то имеем скалярный вектор **A**, т. е. случай 1. Если $a_0 \neq 0$ или $a_2 \neq 0$, то из третьего или первого уравнения системы (3) следует $x_1 = 0$, причем второе уравнение системы (3) задает связь между координатами x_0 и x_2 вида $x_2 = a_2 a_0^{-1} x_0$ или $x_0 = a_0 a_2^{-1} x_2$, соответственно. Поскольку координата $x_3 \in GF(p)$ может принимать произвольные значения при любых значениях остальных координат, приходим к заключению, что множество $\Psi_{\mathbf{A}}$ включает p^2 различных векторов и описывается формулой

$$\mathbf{X} = (x_0, x_1, x_2, x_3) = \left(j, 0, \frac{a_2}{a_0} j, k \right), \qquad (6)$$

где $j, k = 0, 1, 2, \ldots, p-1$, если $a_0 \neq 0$, и формулой

$$\mathbf{X} = (x_0, x_1, x_2, x_3) = \left(\frac{a_0}{a_2} j, 0, j, k \right), \qquad (7)$$

если $a_2 \neq 0$.

Легко показать, что утверждения 1, 2 и 3 сохраняют силу и для случая $a_1 = 0$. Утверждение 2 обосновывает для алгоритмов ЭЦП [14, 15] со скрытой группой, основанных на трудности решения систем многих квадратных уравнений, положение о том, что использование h векторов из скрытой коммутативной группы определяет $h - 1$ квадратных уравнений, задающих попарную перестановочность указанных векторов, Для выбора поля $GF(p)$ и построения упомянутых алгоритмов ЭЦП важным является значение порядка скрытой группы. Последнее определяется порядком мультипликативной группы коммутативных подалгебр, содержащихся в КНАА, используемой в качестве алгебраического носителя. В связи с этим представляет интерес определить число обратимых векторов в коммутативных подалгебрах, содержащихся в рассматриваемой алгебре кватернионов **k**-типа. Для решения этой задачи требуется получить условие обратимости векторов.

Вектор **A** обратим, если векторное уравнение **XA** = **A** имеет решение. Это уравнение сводится к следующей системе из четырех линейных уравнений:

$$\begin{cases} x_0 a_3 - x_1 a_2 + x_2 a_1 + x_3 a_0 = 0; \\ \lambda x_0 a_2 + x_1 a_3 - \lambda x_2 a_0 + x_3 a_1 = 0; \\ x_0 a_1 - x_1 a_0 + x_2 a_3 + x_3 a_2 = 0; \\ \lambda x_0 a_0 + x_1 a_1 - \lambda x_2 a_2 + x_3 a_3 = 1. \end{cases} \qquad (8)$$

Рассмотрим главный определитель системы (8):

$$\Delta = \begin{vmatrix} a_3 & -a_2 & a_1 & a_0 \\ \lambda a_2 & a_3 & -\lambda a_0 & a_1 \\ a_1 & -a_0 & a_3 & a_2 \\ \lambda a_0 & a_1 & -\lambda a_2 & a_3 \end{vmatrix} =$$

$$= a_3 \begin{vmatrix} a_3 & -\lambda a_0 & a_1 \\ -a_0 & a_3 & a_2 \\ a_1 & -\lambda a_2 & a_3 \end{vmatrix} + a_2 \begin{vmatrix} \lambda a_2 & -\lambda a_0 & a_1 \\ a_1 & a_3 & a_2 \\ \lambda a_0 & -\lambda a_2 & a_3 \end{vmatrix} +$$

$$+ a_1 \begin{vmatrix} \lambda a_2 & a_3 & a_1 \\ a_1 & -a_0 & a_2 \\ \lambda a_0 & a_1 & a_3 \end{vmatrix} - a_0 \begin{vmatrix} \lambda a_2 & a_3 & -\lambda a_0 \\ a_1 & -a_0 & a_3 \\ \lambda a_0 & a_1 & -\lambda a_2 \end{vmatrix} =$$

$$= a_3^2 \left(-\lambda a_0^2 - a_1^2 + \lambda a_2^2 + a_3^2 \right) +$$

$$+ \lambda a_2^2 \left(-\lambda a_0^2 - a_1^2 + \lambda a_2^2 + a_3^2 \right) +$$

$$+ a_1^2 \left(\lambda a_0^2 + a_1^2 - \lambda a_2^2 - a_3^2 \right) -$$

$$- \lambda a_0^2 \left(-\lambda a_0^2 - a_1^2 + \lambda a_2^2 + a_3^2 \right) =$$

$$= \left(-\lambda a_0^2 - a_1^2 + \lambda a_2^2 + a_3^2 \right)^2.$$

Система (8) имеет единственное решение, если $\Delta \neq 0$, т. е. получаем следующее условие обратимости вектора **A**:

$$-\lambda a_0^2 - a_1^2 + \lambda a_2^2 + a_3^2 \neq 0. \qquad (9)$$

Условием необратимости вектора **A** является следующее равенство:

$$-\lambda a_0^2 - a_1^2 + \lambda a_2^2 + a_3^2 = 0. \qquad (10)$$

По условию (10) в множестве (5) необратимыми являются векторы, для которых значения j и k удовлетворяют условию

$$k^2 = j^2 \frac{\lambda a_0^2 + a_1^2 - \lambda a_2^2}{a_1^2}. \qquad (10)$$

Если значение $\varepsilon = \dfrac{\lambda a_0^2 + a_1^2 - \lambda a_2^2}{a_1^2}$ является квадратичным невычетом в $GF(p)$, то (5) содержит единственный необратимый вектор **O** = (0, 0, 0, 0) и мультипликативная группа Γ_1 алгебры $\Psi_{\mathbf{A}}$ имеет порядок, равный

$$\Omega_1 = p^2 - 1, \qquad (11)$$

и является изоморфной полю $GF(p^2)$. Это первый тип (тип Γ_1) коммутативных подалгебр $\Psi_{\mathbf{A}}$. Очевидно, группа Γ_1 является циклической.

Если значение ε является квадратичным вычетом в $GF(p)$, то (5) содержит $2p-2$ необратимых векторов, координаты которых соответствуют парам ненулевых значений j и k, удовлетворяющих условиям $j = k$ и $j = -k$, и нулевой вектор **O**, т. е. всего $2p-1$ необратимых векторов. В этом случае порядок мультипликативной группы Γ_1 алгебры $\Psi_{\mathbf{A}}$ имеет порядок, равный

$$\Omega_2 = p^2 - (2p-1) = (p-1)^2. \qquad (12)$$

Эта подалгебра $\Psi_{\mathbf{A}}$ относится ко второму типу (тип Γ_2). Группа Γ_2 порождается двумя образующими одинакового порядка, равного $p-1$. Группы такого типа называются группами с двухмерной цикличностью [16].

Если $\varepsilon = 0$, то в множество (5) необратимыми являются векторы, координаты которых соответствуют всевозможным значениям j при $k = 0$, т. е. всего p векторов, включая нулевой вектор **O**. В этом случае порядок мультипликативной группы Γ_3 алгебры $\Psi_{\mathbf{A}}$ имеет порядок, равный

$$\Omega_3 = p^2 - p = p(p-1). \qquad (13)$$

Эта подалгебра $\Psi_{\mathbf{A}}$ относится к третьему типу (тип Γ_3). Легко показать, что группа Γ_3 является циклической.

В случае подалгебр $\Psi_{\mathbf{A}}$, описываемых формулами (6) и (7), аналогичное рассмотрение числа обратимых и необратимых векторов при различных значениях координат a_0 и a_2 также приводит к подалгебрам типов Γ_1, Γ_2 и Γ_3. Для установления общего числа η подалгебр всех трех типов докажем следующее утверждение.

Утверждение 4. Любой вектор **A**, отличный от скалярного вектора, входит в уникальную коммутативную подалгебру порядка p^2, а именно в подалгебру $\Psi_{\mathbf{A}}$.

Доказательство. В силу утверждения 1, вектор **A**, входящий в подалгебру Ψ, порождает эту подалгебру, т. е. $\Psi = \Psi_{\mathbf{A}}$.

Утверждение 5. Число коммутативных $\Psi_{\mathbf{A}}$-подалгебр порядка p^2 равно $\eta = p^2 + p + 1$.

Доказательство. Каждая $\Psi_{\mathbf{A}}$-подалгебра включает все скалярные векторы число которых равно p. Все другие векторы входят только в одну из $\Psi_{\mathbf{A}}$-подалгебр, поэтому $\eta(p^2 - p) = p^4 - p$, откуда получаем:

$$\eta = p^2 + p + 1. \qquad (14)$$

Применяя способ, предложенный в [17] для вычисления порядка мультипликативной группы конечной алгебры кватернионов, можно доказать, что для рассматриваемой кватернионоподобной алгебры имеет место следующее утверждение.

Утверждение 6. Число обратимых векторов в рассматриваемой кватернионоподобной КНАА **k**-типа равно $\Omega = p(p-1)(p^2-1)$.

При выборе скрытой группы некоторого типа важным является наличие большого числа групп заданного типа. Это обусловливает интерес к вопросу оценки числа групп типов Γ_1, Γ_2 и Γ_3. Пусть переменные η_1, η_2 и η_3 обозначают число групп первого, второго и третьего типов. В соответствии с (14) имеем $\eta_1 + \eta_2 + \eta_3 = \eta$. Число обратимых векторов, отличных от скалярных векторов (число последних равно $p-1$), в рассматриваемой алгебре равно $\Omega - (p-1)$. Число обратимых векторов, отличных от скалярных векторов, содержащихся в группе Γ_i ($i = 1, 2, 3$) равно η_i $(\Omega_i - (p-1))$. Приравнивая различные представления числа одних и тех же векторов, получаем следующее Диофантово уравнение с неизвестными η_1, η_2 и η_3:

$$\eta_1(\Omega_1 - (p-1)) + \eta_2(\Omega_2 - (p-1)) + \\ + \eta_3(\Omega_3 - (p-1)) = \Omega - (p-1). \qquad (15)$$

Выражая значения Ω_1, Ω_2, Ω_3 и Ω через p и выполняя упрощение уравнения (15), с учетом уравнения (14) получаем следующую систему из двух Диофантовых уравнений с тремя целочисленными неизвестными:

$$\begin{cases} \eta_1 + \eta_2 + \eta_3 = \eta; \\ \eta_1 p + \eta_2(p-2) + \eta_3(p-1) = p\left(p^2-1\right) - 1. \end{cases} \qquad (16)$$

Легко показать, что система (1) имеет в целых числах единственное решение, однако, как его найти, является неочевидным. Подсказку дают результаты работы [18] по исследованию строения одной четырехмерной КНАА, заданной по прореженной ТУБВ. В [18] показано наличие подалгебр типов Γ_1, Γ_2 и Γ_3 и установлено число подалгебр каждого типа. Подставляя значения η_1, η_2 и η_3, выраженные через p по формулам из [18], в систему (16), можно установить справедливость следующих выражений, приводимых в [18], также и для исследованной кватернионоподобной КНАА:

$$\eta_1 = \frac{p(p-1)}{2}; \qquad (17)$$

$$\eta_2 = \frac{p(p+1)}{2}; \qquad (18)$$

$$\eta_3 = p+1. \qquad (19)$$

Формулы (17)—(19) показывают, что число коммутативных групп типа Γ_1 и Γ_2 значительно больше (примерно в p раз), чем групп типа Γ_3. Поэтому в качестве скрытой группы в алгоритмах ЭЦП (как основанных на скрытой задаче дискретного логарифмирования, так и основанных на вычислительной трудности решения систем многих квадратных уравнений) следует использовать группы типа Γ_1 и Γ_2.

Строение кватернионоподобных алгебр других типов

Используя метод изучения разбиения КНАА на коммутативные подалгебры, примененный в предыдущем разделе, ко многим кватернионоподобным КНАА типов **e**, **i** и **j**, было установлено, что для них имеет место строение, аналогичное строению, описанному выше. Сформулированные утверждения 1—6 и формулы (11)—(19) сохраняют силу.

Рассмотрим отдельные результаты изучения строения кватернионоподобных КНАА других типов. Для КНАА **e**-типа, заданной по табл. 7, множество векторов входящих в подалгебру $\Psi_{\mathbf{A}}$, порождаемую вектором $\mathbf{A} = (a_0, a_1, a_2, a_3)$, в случае $a_3 \neq 0$ описывается следующей формулой:

$$\mathbf{X} = (x_0, x_1, x_2, x_3) = \left(j, \frac{a_1}{a_3} k, \frac{a_2}{a_3} k, k \right). \qquad (20)$$

При этом условие необратимости вектора **A** имеет вид

$$a_0^2 - \lambda a_1^2 - a_2^2 + \lambda a_3^2 = 0. \qquad (21)$$

Таблица 7

Частный вариант КНАА e-типа

•	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$-\mathbf{e}_3$	$-\lambda\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$-\mathbf{e}_1$	$-\lambda\mathbf{e}_0$

Для КНАА **i**-типа, заданной по табл. 8, множество векторов входящих в подалгебру $\Psi_{\mathbf{A}}$, порождаемую вектором **A**, в случае $a_0 \neq 0$ описывается следующей формулой:

$$\mathbf{X} = (x_0, x_1, x_2, x_3) = \left(j, k, \frac{a_2}{a_0} j, \frac{a_3}{a_0} j \right). \qquad (22)$$

Условие необратимости вектора **A** имеет вид

$$\lambda a_0^2 + a_1^2 - \lambda a_2^2 - a_3^2 = 0. \qquad (23)$$

Таблица 8

Частный вариант КНАА i-типа

•	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$-\lambda\mathbf{e}_1$	$\mathbf{e}_0$	$\lambda\mathbf{e}_3$	$-\mathbf{e}_2$
$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_2$	$-\lambda\mathbf{e}_3$	$\mathbf{e}_2$	$\lambda\mathbf{e}_1$	$-\mathbf{e}_0$
$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_1$

Для КНАА **j**-типа, заданной по табл. 9, множество векторов входящих в подалгебру $\Psi_{\mathbf{A}}$, порождаемую вектором **A**, в случае $a_1 \neq 0$ описывается следующей формулой:

$$\mathbf{X} = (x_0, x_1, x_2, x_3) = \left(\frac{a_0}{a_1} j, j, k, \frac{a_3}{a_1} j \right). \qquad (24)$$

Условие необратимости вектора **A** имеет вид

$$\lambda a_0^2 + a_1^2 - a_2^2 - \lambda a_3^2 = 0. \qquad (25)$$

Таблица 9

Частный вариант КНАА j-типа

•	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\lambda\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\lambda\mathbf{e}_1$
$\mathbf{e}_1$	$-\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_1$	$-\mathbf{e}_0$
$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$-\lambda\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_3$	$-\lambda\mathbf{e}_2$

Заключение

Выполненное исследование декомпозиции кватернионоподобных КНАА различных типов на коммутативные подалгебры показало достаточно полное сходство их строения и потенциальную их применимость в качестве алгебраического носителя алгоритмов ЭЦП со скрытой группой.

Сравнение с результатами исследования [9, 10, 18] четырехмерных КНАА с глобальной двухсторонней единицей, заданных по различным прореженным ТУБВ, показывает, что, видимо, имеет

место общее сходство разбиения на коммутативные подалгебры для четырехмерных КНАА, содержащих единичный вектор указанного типа. Представляет интерес проверка этой гипотезы также и для КНАА, предложенных в статьях [19, 20], однако это представляет предмет отдельного исследования.

Работа выполнена частично в рамках государственного задания Министерства науки и высшего образования Российской Федерации № 075-01024-21-02 от 29.09.2021 (проект FSEE-2021-0015) и при частичной поддержке бюджетной темы № FFZF-2022-0007.

Литература

1. Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms [Электронный ресурс]. Режим доступа: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (дата обращения: 11.04.2022).

2. *Alagic G., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D., Liu Y.* (2019), Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8240, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303 (дата обращения: 11.04.2022).

3. *Moody D., Alagic G., Apon D., Cooper D., Dang Q., Kelsey J., Liu Y., Miller C., Peralta R., Perlner R., Robinson A., Smith-Tone D., Alperin-Sheriff J.* (2020), Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8309 (дата обращения: 11. 04.2022).

4. *Moody D.* (2021) NIST Status Update on the 3rd Round, [online], https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf (дата обращения: 11. 04.2022).

5. *Молдовян Н. А., Абросимов И. К.* Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23—32.

6. *Moldovyan N. A., Moldovyan A. A.* Candidate for practical post-quantum signature scheme // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2020. Т. 16. Вып. 4. С. 455—461. https://doi.org/10.21638/11701/spbu10.2020.410.

7. *Молдовян Д. Н., Молдовян А. А., Молдовян Н. А.* Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах // Вопросы кибербезопасности. 2022. № 1(47). С. 18—25. DOI: 10.21681/2311-3456-2022-1-18-25.

8. *Молдовян Д. Н.* Задание шестимерных алгебр как носителей криптосхем, основанных на скрытой задаче дискретного логарифмирования // Вопросы защиты информации. 2021. № 1. С. 26—32. DOI: 10.52190/2073-2600_2021_1_26.

9. *Moldovyan D. N.* A practical digital signature scheme based on the hidden logarithm problem // Computer Science J. Moldova. 2021. V. 29. № 2(86). P. 206—226.

10. *Moldovyan N. A., Moldovyan A. A.* Digital signature scheme on the 2x2 matrix algebra // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2021. Т. 17. Вып. 3. С. 254—261.

11. *Moldovyan N. A.* Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions // Quasigroups and Related Systems. 2018. V. 26. № 2. P. 263—270.

12. *Moldovyan N. A.* Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. № 2(93). P. 62—67. DOI: https://doi.org/10.21638/11701/spbu10.2021.303.

13. *Moldovyan D. N., Moldovyan N. A.* A post-quantum digital signature scheme on groups with four-dimensional cyclicity // Информационно-управляющие системы. 2021. № 2. С. 43—51. DOI: 10.31799/1684-8853-2021-2-43-51.

14. *Молдовян Д. Н., Молдовян А. А.* Алгебраические алгоритмы ЭЦП, основанные на трудности решения систем уравнений // Вопросы кибербезопасности. 2022. № 2(48). С. 7—17. DOI: 10.21681/2311-3456-2022-2-7-17.

15. *Молдовян Д. Н.* Типовые проверочные уравнения в алгебраических алгоритмах ЭЦП со скрытой группой // Вопросы защиты информации. 2022. № 1. С. 31—37. DOI: 10.52190/2073-2600_2022_1_31.

16. *Moldovyan N. A.* Fast signatures based on non-cyclic finite groups // Quasigroups and Related Systems. 2010. V. 18. № 1. P. 83—94.

17. *Moldovyan D. N.* Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes // Quasigroups and Related Systems. 2010. V. 18. № 2. P. 165—176.

18. *Moldovyan D. N., Moldovyan A. A., Moldovyan N. A.* Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Systems. 2022. V. 30. № 1. P. 133—140.

19. *Абросимов И. К., Ковалева И. В., Молдовян Н. А.* Постквантовый протокол бесключевого шифрования // Вопросы защиты информации. 2017. № 3. С. 3—13.

20. *Moldovyan D. N.* New Form of the Hidden Logarithm Problem and Its Algebraic Support // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. № 2(93). P. 3—10.

Finite quaternion-like algebras as carriers of post-quantum digital signature algorithms

A. A. Moldovyan, D. N. Moldovyan
St. Petersburg Electrotechnical Univeristy "LETI", St. Petersburg, Russia

N. A. Moldovyan, A. A. Kostina
St. Petersburg Federal Research Center of the RAS (SPC RAS), St. Petersburg, Russia

The decomposition of finite four-dimensional associative algebras, the non-commutativity of the multiplication operation in which is given by the asymmetric distribution of a structural constant, into commutative subalgebras is considered. The types of subalgebras and the values of the orders of their multiplicative groups are determined. The results obtained show the possibility of using the studied four finite quaternion-like algebras as carriers of post-quantum digital signature algorithms with a hidden group, including those based on the computational difficulty of finding a solution to a system of many quadratic equations with many unknowns.

Keywords: information security, post-quantum cryptography, digital signature, finite associative algebra, non-commutative algebra, cyclic group, two-dimensional cyclicity.

Bibliography — 22 references. *Received May 6, 2022*

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 003.26
DOI: 10.52190/2073-2600_2022_2_30
EDN: JUHDKM

Использование систем искусственного интеллекта при обеспечении информационной безопасности на объектах критически важной информационной инфраструктуры

В. В. Кабаков
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Особенную актуальность вопросы обеспечения информационной безопасности приобретают для объектов критически важной информационной инфраструктуры. В рамках данной статьи производится анализ актуальности и необходимости обеспечения информационной безопасности на объектах критически важной информационной инфраструктуры. Автором отдельно рассматривается вопрос, связанный с использованием технологии искусственного интеллекта при решении данных задач в отрасли электроэнергетики. Практическая значимость заключается в возможности использования полученных данных при разработке методического обеспечения, регламентирующего защиту данных объектов.

Ключевые слова: информационная безопасность, искусственный интеллект, информационная инфраструктура, защита, доступ.

Энергетическая промышленность представляет колоссальную актуальность на сегодняшний день, посредством которой обеспечиваются электроэнергией гражданские и промышленные объекты. Неотъемлемой частью современных энергетических объектов является синхронизация данных и их информационное сопровождение. С каждым годом растет потребность в информационном обеспечении и потребности в высококачественных средствах защиты информации и безопасности данных [1].

Для решения этой проблемы необходимо использовать высокоэффективную систему защиту информации энергетических объектов, позволяющую вовремя обнаружить проблемы и своевременно принять меры по обслуживанию. В рамках представленной работы более подробно освещается вопрос, связанный с защитой информации на критически важных объектах информационной инфраструктуры электроэнергетической отрасли, основанной на использовании технологии искусственного интеллекта.

Кабаков Виталий Валериевич, старший преподаватель кафедры 104.
E-mail: ser-kvv73@mail.ru

Статья поступила в редакцию 6 апреля 2022 г.

Методы

Автором используются теоретические и эмпирические методы исследования. С целью получения более подробной информации и актуальных данных в работе используются научные работы отечественного и зарубежного авторства. В результате работы автором используются научные материалы таких авторов, как: Зудинов А. С., Бойченко О. В., Аношкина А. А., Artyukhin A. A., Slavutsky A. L., Дячук В. С. и других. В каждой из данных работ затрагиваются фундаментальные вопросы, необходимые с целью воспроизведения общего анализа, касающегося обеспечения защиты информации на критически важных объектах информационной инфраструктуры.

Таким образом, в используемой автором настоящей статьи литературе раскрываются такие вопросы, как: объекты критической информационной инфраструктуры; защита информации на объектах критической информационной инфраструктуры; обеспечение безопасности критически

важных объектов инфраструктуры Российской Федерации; комплексный подход к моделированию системы защиты данных в электроэнергетике и некоторые другие.

Актуальность обеспечения информационной безопасности на критически важных объектах информационной инфраструктуры

Цифровые и информационные технологии (ИТ) — это важнейшая часть современных систем управления, находящихся во всех отраслях экономики на сегодняшний день. Следствием данного фактора является появление новых киберугроз и кибератак, совершаемых в областях, в основе которых функционируют различные информационные системы и иные информационные технологии. В современном мире складывается тенденция роста количества попыток совершения киберпреступлений на объектах критически важной информационной инфраструктуры (КИИ) из области энергетики с помощью использования информационно-коммуникационных технологий (ИКТ).

Российская Федерация является одной из развитых стран у которой энергетика остаётся на высоком уровне развития. Поэтому энергетическим объектам инфраструктуры, которая завязана в одну локальную сеть также нуждается в эффективной системе безопасности. Безопасностью энергетической сферы занимается большое количество высококвалифицированных специалистов в области защиты информации. Комплекс мер применяемых для обеспечения безопасности также должен фиксироваться во времени. Однако одной лишь фиксации по времени недостаточно. В государственном секторе связано с вопросом безопасности более важную роль играет в документооборот [2].

Множественные удачные попытки подобного рода преступлений свидетельствуют о том, что посредством ИКТ действительно можно нанести колоссальный как физический, так и информационный ущерб. Необходимо отметить, что при нахождении киберпреступником уязвимости в одном из компонентов информационной системы на критически важных объектах, представляется возможным осуществление целенаправленных нападений на объекты по всему миру. Исходя из этого, на современных объектах КИИ особую актуальность приобретают задачи, решение которых направлено на своевременное обновление базовых компонентов систем управления. Также стоит отметить, что на сегодняшний день не только со стороны производителей, но и со стороны самих потребителей не всегда уделяется должное внимание вопросу кибербезопасности. Совокупность данных факторов приводит к развитию новых методов и угроз нарушения безопасности.

Актуальность использования интеллектуальных технологий при решении трудно-вычислимых задач

Развитие информационных технологий имеет весомый вклад при решении профессиональных задач в современной человеческой жизнедеятельности. Особенно актуальным становится вопрос использования технологии искусственного интеллекта (ИИ) и машинного обучения при решении различных прикладных задач. Технологии искусственного интеллекта представляют высокую актуальность в рамках современного технологического прогресса. В Российской Федерации на сегодняшний день производятся активные инвестиции в рынок развития интеллектуальных средств, суммарно составляющих порядка 140 млн долл. (рис. 1) [3].

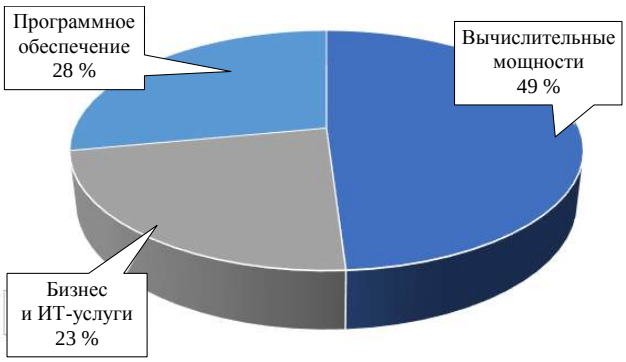


Рис. 1. Распределение инвестиций в рынок ИИ

Ключевым инструментом повышения эффективности и рациональности работы информационных технологий при решении различных задач является разработка интеллектуальных средств, способных самообучаться и решать трудно-вычислимые задачи, работая с большим объемом данных.

Обеспечение информационной безопасности объектов КИИ посредством использования технологии искусственного интеллекта

Критическая информационная инфраструктура энергетического предприятия представляет из себя набор информационных систем и различных си-

стем автоматизированного управления. Помимо этого, в состав КИИ энергетики также входят и сети электросвязи, которые используются с целью организации их взаимодействия. Компьютерная атака на объекты критически важной информационной инфраструктуры расцениваются как целенаправленное воздействие на объекты, направленные на нарушение или же полное прекращение функционирование КИИ [4].

Одним из наиболее перспективных и актуальных инструментов обеспечения кибербезопасности объектов КИИ является технология искусственного интеллекта. Посредством интеллектуальных средств представляется возможность производить анализ большого объема данных с быстрой скоростью. Именно это и позволяет обнаруживать угрозы кибербезопасности и прогнозировать их в дальнейшем посредством самообучения модели ИИ и моделирования рисков в целом. На сегодняшний день существует ряд интеллектуальных решений применительно к кибербезопасности (рис. 2) [5, 6].

Технологии искусственного интеллекта самообучаются на миллиардах потоков данных, совершенствуя свои знания и "понимая" угрозы и риски для кибербезопасности. ИИ выполняет анализ взаимосвязей колоссального количества данных в считанные секунды, посредством чего аналитики намного быстрее реагирую на угрозы относительно традиционных инструментов. ИИ избавляет от длительных исследований и предоставляет уже готовый анализ рисков, сокращая время, необходимое аналитикам для принятия ключевых решений и согласованного устранения угрозы [7].

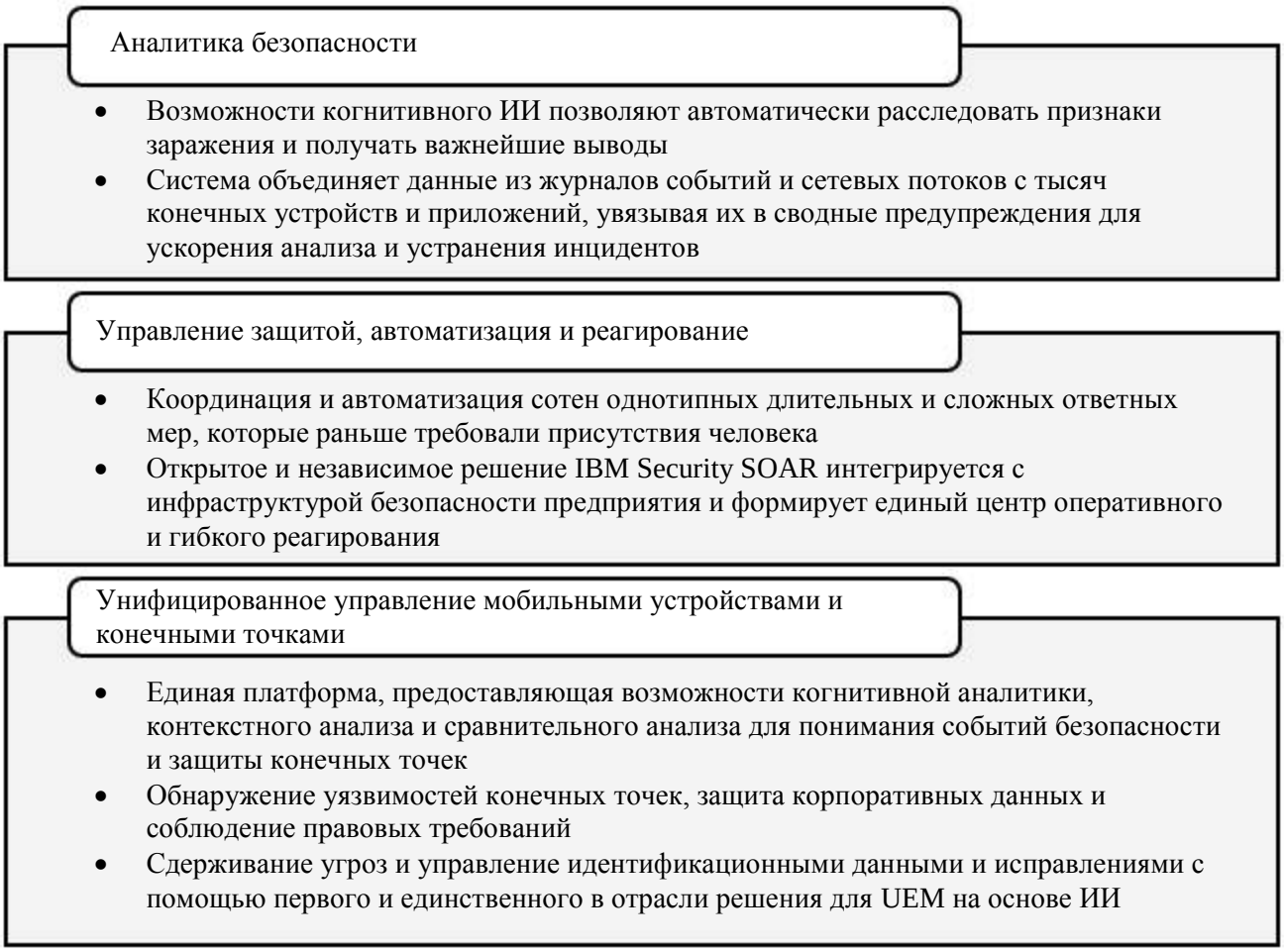


Рис. 2. Решения ИИ для кибербезопасности

Заключение

Таким образом, основной целью данной статьи являлось изучение вопроса обеспечения информационной безопасности объектов КИИ, основанного на использовании интеллектуальных технологий. В рамках представленной статьи были рассмотрены такие аспекты, как: актуальность обеспечения информационной безопасности на объектах электроэнергетики; актуальность и необходимость использования интеллектуальных технологий при защите информации на объектах КИИ; инструменты и результаты возможного использования ИИ при решении данных задач.

В заключение необходимо отметить, что обеспечение ИБ — это одно из самых актуальных направлений в современном ИТ-секторе. Это является следствием тотальной цифровизации современного общества и промышленности. На сегодняшний день различными образовательными организациями ежегодно выпускаются тысячи квалифицированных специалистов, деятельность которых напрямую связана с работой с цифровыми технологиями или же обеспечением информационной безопасности информационных объектов. Одним из наиболее актуальных направлений из области защиты информации является обеспечение ИБ на объектах критически важной информационной инфраструктуры электроэнергетики.

Литература

1. *Зудинов А. С.* Защита информации на объектах критической информационной инфраструктуры // StudNet. 2021.
2. *Бойченко О. В., Аношкина А. А.* Обеспечение безопасности критически важных объектов инфраструктуры Российской Федерации // Ученые записки Крымского федерального университета имени В. И. Вернадского. Экономика и управление. 2016.
3. *Kosheev M. I., Artyukhin A. A., Slavutsky A. L.* The use of adaptive neuroalgorithms for the recognition of abnormal modes of secondary power equipment systems // Bulletin of ChSU. 2019.
4. *Оюн Ч. О., Попантонопуло Е. В.* Объекты критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. 2018.
5. *Erokhin S. D., Petukhov A. N., Pilyugin P. L.* Principles and tasks of asymptotic security management of critical information infrastructures // T-Comm. 2019.
6. Дубинин Д. П. Использование доверительных систем с целью обеспечения информационной безопасности и ограничения несанкционированного доступа для информационных систем финансовых организаций // Вопросы защиты информации. 2022. № 1(136). С. 3—6.
DOI 10.52190/2073-2600_2022_1_3. — EDN QTWDVT.
7. *Дячук В. С.* Комплексный подход к моделированию системы защиты данных в электроэнергетике // Ученые записки Крымского федерального университета имени В. И. Вернадского. Экономика и управление. 2016.

The use of artificial intelligence systems in ensuring information security at critical information infrastructure facilities

V. V. Kabakov
Moscow Aviation Institute (National Research University), Moscow, Russia

The issues of ensuring information security are of particular relevance for objects of critical information infrastructure. Within the framework of this article, the analysis of the relevance and necessity of ensuring information security at the objects of critical information infrastructure carried out. The author separately considers the issue related to the use of artificial intelligence technology in solving these problems. The practical significance lies in the possibility of using the data obtained in the development of methodological support regulating the protection of these objects.

Keywords: information security, artificial intelligence, information infrastructure, protection, access.

Bibliography — 7 references. *Received April 6, 2022*

УДК 004
DOI: 10.52190/2073-2600_2022_2_34
EDN: JZYGFG

Защищенные информационные технологии в цифровой экономике

В. А. Конявский, д-р техн. наук
Московский физико-технический институт (национальный исследовательский университет), г. Долгопрудный, Московская обл., Россия

В. В. Медведев, канд. экон. наук
АНО ВО "Российский новый университет", Москва, Россия

Г. В. Росс, д-р экон. наук, д-р техн. наук
Российский экономический университет им. Г. В. Плеханова, Москва, Россия

Открытые информационные системы активно внедряются в жизнь, растет актуальность защиты в таких системах, но в то же время подавляющее число подходов ориентировано только на корпоративные системы. В статье рассматриваются особенности защиты информации в открытых системах, характерных для цифровой экономики. Показано, что необходимо учитывать требования по защите информационных технологий, рассматриваемых как последовательность операций. Для этого предложен механизм трейлеров безопасности, рассмотрены условия эквивалентности информационных технологий. Решена задача выбора маркеров и их агрегирование для случаев распределенных информационных систем, включающих недоверенные подсистемы.

Ключевые слова: информационные технологии, цифровая экономика, защищенные информационные технологии, граф.

Давно и хорошо известно, как обеспечить достаточный уровень защищенности в системах, для которых известен состав технических средств, потоки данных и их характеристики, перечислены участники системы и есть надежные способы их идентификации с применением доверенных компьютерных средств (СВТ) и систем. Такие системы являются корпоративными, и для корпоративных систем создать надежную систему защиты в этих условиях возможно.

С переходом к цифровой экономике все радикально изменилось.

Системы преимущественно становятся открытыми — а сделать защищенными все СВТ в открытой системе — невозможно.

Обеспечение достаточного уровня защищенности в открытых системах — новая задача. Теперь нельзя опираться на доверенность СВТ. В некоторых случаях можно использовать специальные информационные технологии, которые могут помочь обеспечить требуемый уровень доверия при использовании недоверенных технических средств [1], однако примеров таких технологий пока весьма немного.

Очевидно, что наступило время радикально изменить подход — например, базируясь на имеющихся в реальной жизни примерах. Так, денежные купюры изготавливаются с помощью защищенных технологий на доверенных производствах, но обращаются в незащищенной и агрессивной среде. И при этом, как правило, не возникает существенных сложностей с идентификацией подлинных и поддельных банкнот. В этом помогают специальные метки, которые вводятся в банкноту в процессе ее изготовления.

Итак — специальные метки, обеспечивающие безопасность, внедряются в доверенном производстве, а используются при свободном движении в агрессивной внешней среде. Суть таких меток — служить индикаторами выполнения тех или иных производственных операций. Метка — как бы "прицеп" к операции, "трейлер безопасности". Их совокупность может дать основания считать продукт, функционирующий в агрессивной среде, подлинным или фальшивым. В сфере материального производства такие методы хорошо известны, и производство банкнот — не единственный пример. Основываясь на опыте материального производства, можно предложить аналогичные подходы для информационного производства.

Конявский Валерий Аркадьевич, заведующий кафедрой "Защита информации".
E-mail: konyavskiy@gospochta.ru
Медведев Вадим Викторович, доцент кафедры "Государственное и муниципальное управление".
E-mail: in.medvedeva@hotmail.com
Росс Геннадий Викторович, главный научный сотрудник.
E-mail: ross-49@mail.ru

Статья поступила в редакцию 15 июня 2022 г.

Рассмотрим базовые понятия, касающиеся отношений в сфере материального производства, и посмотрим, можно ли их использовать для решения наших задач.

А. Доверенные системы. Базовые понятия

В соответствии с [2]:

1. Производство — процесс создания какого-либо продукта.

2. Технология, технологический процесс — последовательность операций преобразования материалов в продукцию[1].

3. Технологическая операция — это законченная часть технологического процесса, выполняемая на одном рабочем месте.

Перейдем теперь к информационным технологиям (ИТ). На наш взгляд, они не сильно, в концептуальном смысле, отличаются от технологий в материальном производстве.

Мы возьмём за основу традиционные определения в сфере материального *производства*, проверенные временем и опытом, и на этой основе определим объекты и процессы информационного производства.

4. Информационное производство — производство электронных документов (ЭлД) и управляющих сигналов [2].

Особым классом информационных систем (ИС) являются системы управления производственными процессами [3]. При этом управляющие сигналы влияют на производственные так, как электронный документ влияет на свой сектор действенности [4, С. 106—110]. В силу этого определение можно считать верным.

5. Информационная технология — последовательность информационных операций преобразования данных в документы [5].

Для нас важнейшим является именно "последовательность" операций. Изменяя последовательность вычислительных операций, из любых начальных данных можно получить любой результат. Такое преобразование нельзя считать "технологией". Последовательность операций должна быть фиксирована, соответствовать тому, что в материальном производстве называется "технологическая карта".

6. Защищённая информационная технология — ИТ, обладающая свойством сохранять последовательность операций [2, 5].

Б. Информационные технологии как предмет защиты

В процессе информационного взаимодействия участвуют:

- компьютеры;
- сообщения;
- каналы (связи);
- информационные технологии.

Здесь защищенные ИТ — новое направление [5], дополняющее защиту компьютеров, данных и каналов. Здесь защита ИТ позволит обеспечить достаточный уровень защищенности информационного производства в целом.

Возможны различные способы формирования (изготовления) объекта. Соответственно, различными будут описания технологий, позволяющих изготовить идентичные объекты. Идентичность (содержание) двух информационных объектов определяется идентичностью внутренней информации документа. То есть возможно существование различных ИТ, при применении которых будут созданы информационные объекты, несущие сообщение об одном и том же информационном факте.

Очевидно, что основным вопросом в теории защиты ИТ как последовательности информационных операций будет вопрос установления эквивалентности $S_1 \sim S_2$. В качестве примера можно привести поиск эквивалентной структуры вредоносной программы, специфика которой известна заранее [6].

Множество электронных сообщений (электронных документов) можно разделить на группы, например, по уровню конфиденциальности. На основе требований безопасности система определения эквивалентности двух произвольных ИТ будет наполнена некоторым набором правил. Таким образом, множество электронных сообщений (электронных документов) будет разделено на классы, каждый из которых описан уникальной системой правил эквивалентности объектов. Иными словами, будет формироваться вариационное исчисление: полный алфавит — множество операций класса; система эквивалентных преобразований — правила сравнения ИТ.

Используемую технологию информационного обмена можно интерпретировать как некоторую последовательность операций, сформированную на основе выборки с возвращением из базисного множества операций [4].

Очевидно, что для контроля корректности ИТ недостаточно проверки правильности исполнения элементарных операций — на основе "проверенных" операций может быть сформирована некорректная технология — например, изменением последовательности операций.

[1] Здесь уже можно отметить, что продукция явно или неявно несет на себе информацию о технологическом процессе, в котором она (продукция) была изготовлена.

Одним из следствий этого подхода является требование к преобразованиям информации в электронной среде: требование сохранения отношения упорядоченности [7]. Таким образом, единый подход, основанный на установлении эквивалентности, может обеспечить как контроль объектов, так и контроль процессов (технологий).

В. Защита технологии производства электронных документов

Очевидно, что существуют различные виды электронных документов (ЭлД)[1], как и документов вообще. Естественно, что применять сложные и дорогостоящие технологии защиты для малозначительных ЭлД нецелесообразно (принцип необходимости и достаточности средств защиты). Для иллюстрации этого факта можно сравнить необходимые уровни защиты информационного письма, банковского платежного документа, ценных бумаг и документов, содержащих сведения, составляющие государственную тайну. В связи с этим естественно предложить некоторую иерархию трейлеров безопасности (ТБ) [5] для различных видов документов.

При разработке информационной технологии определяется набор допустимых операций [8], в том числе: операции доступа, функциональные, вычислительные, запросы на доступ и др.

Введем обозначение O_i, множества операций i-го типа, $i = \overline{1, m}$.

Рассмотрим множество всех операций ИС как объединение множеств операций различных типов:

$$O = \bigcup_{i=1}^{m} O_i, O_i \cap O_j = \varnothing, i \neq j, \ |O| = |O_1| + \ldots + |O_m| = k.$$

Определение 1. Технологией изготовления (обработки)[2] электронного документа будем называть последовательность операций из множества O, результатом применения которых к исходным сведениям является электронный документ**.**

Каждой операции $o \in O$ поставим в соответствие ТБ, т. е. некоторый реквизит, фиксирующий целостность применения технических и программных средств при выполнении функций обработки исходных сведений.

Обозначим трейлеры безопасности T_i, $i = \overline{1, k}$

Рассмотрим множество всех возможных ТБ:

$$T = \{T_1, \ldots, T_k\} = \{T_i\}_{i=1}^{k}, \ |T| = k.$$

Множество всех возможных *подмножеств* множества T обозначим **T**.

В процессе изготовления электронного документа формируется последовательность ТБ, соответствующих операциям, входящим в состав технологии изготовления ЭлД.

Обозначим такую последовательность трейлеров безопасности T, $T \in$ **T**.

Установим связь между технологией изготовления ЭлД и последовательностью T, содержащейся в ЭлД.

Определение 2. Электронный документ — это сведения в электронном виде в совокупности с последовательностью ТБ, соответствующей технологии изготовления ЭлД:

$$\text{ЭлД} = \{\textit{Сведения, } T\}.$$

Последовательностью ТБ фиксируют целостность документа и неизменность технологии на протяжении технологического процесса изготовления ЭлД. Таким образом, ТБ являются специфическими элементами, несущими в себе информацию о подлинности рассматриваемого электронного документа.

Данное свойство ТБ можно использовать для решения вопроса подлинности ЭлД.

Предположим существование в ИС некоторого ЭлД, подлинность которого необходимо установить:

$$\text{ЭлД}^* = \{\textit{Сведения}^*, T^*\},$$

где $T^* = \{T_1^*, \ldots, T_p^*\}$, $T_i^* \in T$, $i = \overline{1, p}$.

Каждый из ТБ, входящий в последовательность T^*, соответствует некоторой операции $o \in O$ и является реквизитом, фиксирующим целостность выполнения операции применительно к исходным сведениям.

В процессе создания ЭлД на каждом этапе, т. е. при выполнении каждой операции, вычисляется значение ТБ, соответствующего этой операции.

Введем обозначение:

NT_i — значение трейлера безопасности $T_i \in T$, $NT_i \in N$, $i = \overline{1, k}$.

Значение ТБ вычисляется как функция от самого трейлера безопасности (как реквизита, соответствующего некоторой операции $o \in O$) и от сведений, содержащихся в изготавливаемом ЭлД:

[1] В широком смысле — как продукт информационного производства, а не файл с электронной подписью.

[2] Под обработкой можно понимать и изготовление копии ЭлД, так что далее будем использовать термин "изготовление".

$$NT_i = f\ (Сведения,\ T_i).$$

Рассмотрим подробней структуру ТБ. Будем рассматривать ТБ как совокупность некоторой описательной части (назовем ее *Заголовок),* содержащей в себе данные об операции, в соответствие которой поставлен ТБ; функциях, с помощью которых вычисляется ТБ; и значения ТБ:

$$T_i = \{Заголовок\ T_i,\ NT_i\},\ T_i \in T,\ NT_i \in N,\ i = \overline{1, k}$$

Трейлер безопасности T_i = {*Заголовок* T_i, NT_i} с вычисленным значением NT_i включается в обрабатываемый ЭлД. Тогда рассматриваемый ЭлД может быть представлен в следующем виде:

$$ЭлД^* = \{Сведения^*,\ T^*\},$$

где $T^* = \{T_i^*, T_p^*\},\ T_i^* \in T,\ i = \overline{1, p}$ и T_i = {*Заголовок* T_i, NT_i}

Определение 3. ЭлД является подлинным тогда и только тогда, когда подтверждена:

– неизменность технологии изготовления (обработки) ЭлД;

– целостность сведений, входящих в рассматриваемый ЭлД.

Рассмотрим этапы установления подлинности ЭлД.

1. Анализ неизменности (эквивалентности) технологии изготовления (обработки) ЭлД.

Изготовление любого электронного документа заключается в последовательном применении некоторого набора операций к исходным сведениям. Некоторые операции (например, чтение) могут быть использованы как однократно, так и несколько раз. Поскольку каждая произведенная операция фиксируется в ИТ путем установки ТБ, то, например, повторное прочтение данных в процессе изготовления (обработки) ЭлД может трактоваться как некоторое технологическое отличие. Однако в случае, когда повторное использование операции является допустимым, можно говорить об эквивалентности информационных технологий и, соответственно, об эквивалентности изготовленных (обработанных) по ним ЭлД.

Рассмотрим множество информационных ресурсов. Выделим из него множество всевозможных ЭлД.

Обозначим его *D.*

Разобьем множество *D* на подмножества в соответствии с требованиями нормативных документов по защите или требованиями, устанавливаемыми собственником информации.

Обозначим их $D_i, i = \overline{1,l}$, $D = \bigcup_{i=1}^{l} D_i$.

Определение 4. Подмножества D_i, $i = \overline{1,l}$ будем называть классами электронных документов.

На практике возможны различные способы изготовления (обработки) ЭлД, принадлежащих классу D_i. Другими словами, возможно существование различных ИТ, т. е. приемов, способов и методов применения технических и программных средств при выполнении функций обработки исходной информации, результатом которых будет ЭлД из класса D_i.

Каждую из технологий для класса D_i обозначим $T_j^i,\ j = \overline{1, r}$.

Как отмечено выше, каждой технологии изготовления соответствует последовательность ТБ.

Определение 5. Базовой ИТ для класса электронных документов D_i будем называть технологию, которой соответствует последовательность трейлеров безопасности *T* наименьшей длины.

Такую последовательность для каждого класса электронных документов D_i, $i = \overline{1,l}$ обозначим $T_i^б,\ i = \overline{1, l}$.

Далее для каждого класса D_i, $i = \overline{1,l}$ возникает вопрос об эквивалентности информационных технологий $T_j^i, j = \overline{1,r}$.

Рассмотрим множество трейлеров безопасности *T* как алфавит, т. е. как систему попарно различных знаков, T_i — буквы в алфавите *T.*

Последовательность трейлеров безопасности *T* любого ЭлД, т. е. элемент множества **T**, является словом в определенном алфавите *T.*

Согласно [9], преобразование одних слов алфавита в другие осуществляется посредством некоторых допустимых подстановок, которые заданы в виде $R \to Q$, где *R* и *Q* слова в заданном алфавите *T.*

Для рассматриваемого класса электронных документов D_i определим конечную систему допустимых подстановок. Обозначим ее P_i.

Определение 6. Если слово *R* может быть преобразовано в слово *Q* посредством *n*-кратного применения допустимых подстановок, т. е. существует дедуктивная цепочка, ведущая от слова *R* к слову *Q*, то в таком случае слова *R* и *Q* называются эквивалентными: $R \sim Q$.

Ассоциативным исчислением будем называть совокупность всех слов в алфавите вместе с какой-нибудь конечной системой допустимых подстановок.

В нашем случае, для класса D_i ассоциативное исчисление есть {**T**, P_i}.

Как отмечалось выше, T_j^i, $j = \overline{1,r}$ являются словами в алфавите T.

Определение 7. Информационные технологии T_{r1} и T_{r2}, T_{r1}, $T_{r2} \in \mathbf{T}$, будем называть эквивалентными, если соответствующие им последовательности трейлеров безопасности эквивалентны как слова в алфавите T.

Таким образом, вопрос об эквивалентности ИТ будем рассматривать как проблему эквивалентных слов в ассоциативном исчислении $\{\mathbf{T}, P_i\}$, т. е. если из слова T_{r1} путем применения допустимых подстановок из P_i, может быть получено слово T_{r2}, то ИТ являются эквивалентными.

Учитывая все вышесказанное, предположим, что рассматриваемый ЭлД* принадлежит некоторому классу электронных документов.

Обозначим его $D^* \subset D$.

Последовательность трейлеров безопасности T^* рассматриваемого электронного документа ЭлД* соответствует технологии изготовления (обработки) ЭлД*.

Согласно ***определению 5*** класс электронных документов $D^* \subset D$ связан с базовой информационной технологией $T^{*б}$.

Тогда в случае, если информационные технологии T^* и $T^{*б}$ эквивалентны как слова в алфавите T, будем утверждать, что неизменность технологии изготовления (обработки) T^* электронного документа ЭлД* установлена.

Определение 8. ИТ для класса электронных документов будем называть защищенной, если информационные технологии T_j^i, $j = \overline{1,r}$ являются попарно эквивалентными в ассоциативном исчислении $\{\mathbf{T}, P_i\}$.

2. Анализ неизменности сведений, содержащихся в ЭлД.

Для каждого трейлера безопасности T_j^*, $j = \overline{1,p}$, входящего в последовательность T^*, необходимо вычислить значение $NT_j^* = f(Сведения^*, T_j^*)$, $j = \overline{1,p}$ (данные о функции f получены из *Заголовка* T_j^*) и сравнить полученные значения с уже имеющимися значениями NT_j, $j = \overline{1,p}$, из набора трейлеров безопасности T^*. В случае, когда

$$NT_i = NT_j^*, \; i = \overline{1,p}$$

т. е. в случае совпадения всех вычисленных значений трейлеров с уже имеющимися значениями, можно говорить о целостности сведений, содержащихся в ЭлД*.

Таким образом, иерархия защиты ЭлД связана с установлением соответствия:

– классов ЭлД последовательностям $T_i^б$, $i = \overline{1,l}$ (классификация ЭлД по минимальному множеству ТБ, достаточному для защиты этого типа документов);

– информационных технологий ассоциативным исчислениям $\{\mathbf{T}, P_i\}$, $i = \overline{1,l}$ (классификация информационных, технологий по множеству ТБ, которые могут устанавливаться на ЭлД в процессе изготовления, и допустимым подстановкам, учитывающим возможные расхождения в множествах трейлеров безопасности).

Как отмечалось выше, каждой операции в ИС нами ставится в соответствие трейлер безопасности. Тем самым в ИС используется набор трейлеров безопасности T^*.

Множество возможных электронных документов D^* разбивается на подмножества D_i. Каждому подмножеству D_i соответствует базовая информационная технология, т. е. последовательность трейлеров безопасности T_i.

Базовая технология изготовления документов каждого класса содержит минимальное число операций, результатом применения которых к исходным сведениям является ЭлД рассматриваемого класса.

Возникает вопрос, возможно ли изготовление (обработка) ЭлД, принадлежащих некоторому классу электронных документов $D_i \subset D$ в некоторой рассматриваемой информационной системе.

Для решения этого вопроса используются последовательности трейлеров безопасности T^* (соответствующая рассматриваемой системе) и T_i (соответствующая базовой технологии класса электронных документов D_i).

В случае, когда $T_i \subset T^*$, т. е. множество операций включает в себя операции, необходимые для изготовления (обработки) ЭлД D_i, рассматриваемая система может быть использована для работы с электронными документами класса D_i.

Таким образом, используя набор трейлеров безопасности, можно классифицировать ИС в соответствии с заданными классами электронных документов.

В результате информационного производства в ИС производятся электронные документы. Как правило, ИС так или иначе защищены, на уровне, который их владельцы считают достаточным. Границы этих систем известны, как и их состав и структура, и для них меры защиты (как правило, периферийной) хорошо известны. Эти системы и продуцируют ЭлД с некоторым уровнем доверия.

Тем не менее, изготовление ЭлД возможно и с использованием незащищенных компьютеров и ИТ, и, главное, оборот ЭлД осуществляется, как правило, в незащищенной и агрессивной среде.

Методы выбора трейлеров безопасности

Содержательная постановка задачи. Технология обработки электронного документа может быть представлена в виде графа конвейерного типа. Последовательность операций обработки ЭлД жестко задана. Каждой операции изготовления ЭлД поставлены в соответствие несколько вариантов возможных трейлеров безопасности, то есть маркеров, один из которых должен внедряться в технологию обработки ЭлД при выполнении данной операции. Трейлеры безопасности (в дальнейшем будем использовать термин маркер), в общем случае, должны включать в себя набор реквизитов, фиксирующих целостность выполнения операции ЭлД применительно к исходным сведениям. Основной характеристикой маркера является его длина, то есть объем памяти, выделяемый для хранения соответствующего маркера. Зная длину маркера, можно вычислить сопутствующие ему характеристики: затраты на хранение и время передачи, а также возможный уровень обеспечения достоверности. Отсутствие этапа установки маркера может создать условия для возможного нарушения достоверности ЭлД, причем нарушение при отсутствии маркера не будет устанавливаться при проверке.

В этих условиях возникает задача выбора маркеров для каждой операции обработки ЭлД и их агрегирование с целью оптимизации заданного критерия при заданных ограничениях. В качестве функционала цели и ограничений могут выступать перечисленные выше характеристики маркеров [9].

Формальная постановка задачи. Сформулируем постановку задачи в терминах теории графов [10, 11]. Пусть задан линейный взвешенный ориентированный мультиграф $G(X, U)$, в котором X — множество вершин соответствующее состоянию ЭлД $x(i) \in X$, а дуги U — соответствуют различным вариантам расстановки маркеров для реализации операций $(ij) \in U$. В мультиграфе состояния ЭлД $x(i)$ и $x(j)$ будут связаны несколькими дугами $((ij),k) \in U$, где k — номера вариантов установки маркеров, которые различаются объемом выделяемой ему памяти.

Пример 1. На рис. 1 представлен мультиграф, который имеет четыре состояния ЭлД ($x(1)$ $x(2)$ $x(3)$ $x(4)$) и три операции (12), (23), (34), каждая из которых имеет три варианта установки маркеров $(ij)k$ (для операции (12) имеем варианты: (12)1, (12)2, (12)3) и т. д. так для каждой операции.

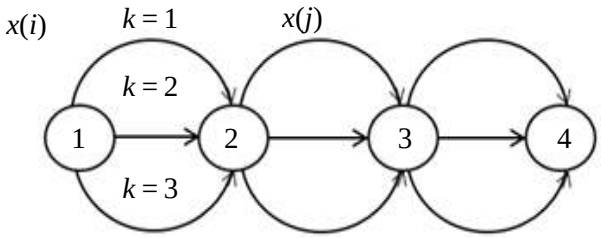


Рис. 1. Мультиграф технологии обработки электронного документа

Присвоим каждой дуге $(ij)k \in U$ три числа: $r1(ij)k$ — объем памяти маркера для (ij)-й операцию, выбранного по k-му варианту, $r2(ij)k$ — уровень обеспечения достоверности маркера (ij)-й операцию, выбранного по k-му варианту $r3(ij)k$ — время передачи маркера (ij)-й операцию, выбранного по k-му варианту, $r4(ij)k$ — затраты на хранения k-го маркера (ij)-й операции. Три последних параметра являются производными от длины маркера и вычисляются следующим образом:

$r2(ij)k = r1(ij)k / P(ij)$, где $P(ij)$ — максимально возможный объем памяти маркера для каждой (ij) — операции;

$r3(ij)k = r1(ij)k \cdot t1$, где $t1$ — время передачи единицы информации.

$r4(ij)k = r1(ij)k \cdot c1$, где $c1$ — затраты на хранения единицы информации.

В этом случае задача обеспечения достоверности обработки ЭлД будет заключаться в оптимизации вариантов проставления маркеров и агрегировании операций в трейлеры безопасности, т. е. в решении двух взаимосвязанных задач, а именно:

- задачи выбора из множества возможных вариантов проставления маркеров оптимального для каждой операции;
- задачи агрегировании операций в трейлеры безопасности и расстановки их на конвейере.

Задача 1. Процедура формализации этой задачи заключается в необходимости преобразовать исходный взвешенный ориентированный мультиграф $G(X, U)$ конвейерного типа (рис. 1) в двудольный граф $G_D(X_D, U_D)$ (рис. 2) [10, 11], множество вершин которого X_D разбито на два непересекающихся подмножества: $X1_D$ соответствует множеству операций, а $X2_D$ — множеству маркеров, причем дуги множества U_D соединяют вершины разных подмножеств ($|X1_D| = m$, $|X2_D| = n$, $|X_D| = m + n$).

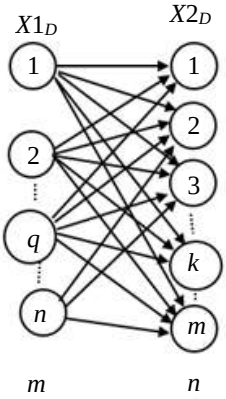


Рис. 2. Двудольный граф $G_D(X_D,U_D)$

Для упрощения описания формальной постановки задачи заменим обозначение номера операции (ij) мультиграфа $G(X, U)$ на индекс q, т. е. $q \in X1_D$ ($q = 1, m$), при этом номера маркеров $k \in X2_D$ ($k = 1, n$). Тогда перепишем все параметры: $r1(qk)$ будет определять объем памяти, выделяемый маркеру для q-й операцию, выбранного по k-му варианту; $r2(qk)$ — уровень обеспечения достоверности маркера q-й операцию, выбранного по k-му варианту; $r3(qk)$ — время передачи маркера q-й операцию, выбранного по k-му варианту; $r4(qk)$ — затраты на хранения k-го маркера q-й операции.

Таким образом, требуется среди дуг множества U_D выбрать такие, чтобы:

1. Все вершины подмножества $X1_D$ были достижимы вершинам подмножества $X2_D$, при этом, каждой вершине подмножества $X1_D$ была инцидентна только одна дуга (рис. 3).

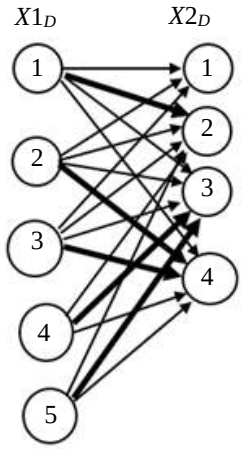


Рис. 3. Двудольный подграф $G_D(X_D^1, U_D^1)$ графа $G_D(X_D,U_D)$ (операция 1 фиксируют целостность документа с помощью 2-го варианта маркера, 2- я и 3-я операции с помощью 4 варианта, а 4- и 5-я с помощью 3 варианта)

2. Суммарное значение параметра, определяющего функционал цели, всех выбранных дуг была бы минимальна.

Реализация этого требования заключается в определении подграфа $G_D(X_D^1, U_D^1)$ (на рис. 3 дуги подграф выделен жирными линиями).

Введем булеву переменная $z(qk)$ равную 1, если q-я операции реализуется с помощью k-го маркера, и 0, в противном случае. Исходными данными к задаче являются: параметры $r1(qk)$, $r2(qk)$, $r3(qk)$, $r4(qk)$ и ограничения на суммарные затраты S, выделенных для формирования набора реквизитов всех маркеров, а также максимальный возможный объем памяти Vq, который может быть выделен под маркеры для каждой q-й операции.

Формальная постановка задачи в этом случае имеет вид [9]:

минимизировать суммарный объем памяти всех маркеров заданного множества операций ЭлД:

$$\sum_{q\in X1_D}\sum_{k\in X2_D} r1(qk)\,z(qk) \Rightarrow \min, \qquad (1)$$

при ограничениях:

суммарные затраты на формирование всех маркеров не должны превышать S

$$\sum_{q\in X1_D}\sum_{k\in X2_D} r4(qk)\,z(qk) \le S \qquad (2)$$

максимальный объем памяти маркера q-й операции не должен превышать Vq

$$\forall q \in X1_D,\ \max_k r1(qk)\,z(qk) \le Vq, \qquad (3)$$

во все операции должны быть включены маркеры

$$\forall q \in X1_D,\ \sum_{k\in X2_D}^{n} z(qk) = 1, \qquad (4)$$

все переменные имеют булевы значения

$$\forall (qk) \in U_D,\ z(qk) = 1,0. \qquad (5)$$

Решением задачи (1)—(4) является выделенный на рис. 3 из графа $G_D(X_D, U_D)$ подграф $G_D(X_D^1, U_D^1)$ минимального веса, причем каждая вершина множества $X1_D$ имеет только одну дугу с множеством $X2_D$.

Пример 2. В табл. 1 представлены параметры $r1(qk)$, в которой строки соответствуют номерам операций, а столбцы — номерам вариантам маркеров, а также столбец Vq, определяющий ограничения на максимальный объем памяти для каждой операции. В табл. 2 представлены откорректиро-

ванные параметры $r1(qk)$ с учетом этого ограничения Vq, т. е. из рассмотрения будут исключены варианты маркеров, которые не соответствуют ограничениям (значение их равно ∞). В табл. 3 заданы затраты $r1(qk)$, выделенные числа исключаются из рассмотрения так как они исключены из матрицы $r4(qk)$, при этом суммарные затраты S не должны превышать, выделенные средств $S < 20$.

Для решения задачи могут быть использованы переборный алгоритм [9], дерева решений которого представлено на рис. 4.

На рис. 4 цифры, стоящие у вершин дерева решений соответствуют их весу: первая цифра определяет текущему значению объема памяти, а в скобках указаны текущее значение затрат на реализацию маркеров. Висячие вершины графа соответствуют бесперспективности продолжения поиска в этом направлении. Оптимальный результат соответствует выбору 3-го варианта расстановки маркеров для всех операций, при этом суммарный объем памяти маркеров — 6 у.е., а суммарные затраты 12 у.е.

Задача 2. Агрегирование маркеров заключается в возможном комплектовании нескольких ТБ, содержащих некоторые виды маркеров, в частном случае ТБ может содержать один вид маркера обработки ЭлД. При этом агрегированные операции должны выполняться на защищенном (доверенном) рабочем месте, стоимость реализация которых достаточно велика.

Представим технологический процесс конвейерного типа в виде ориентированного линейного графа $G(X, U)$, вершины которого отвечают состоянием операции, а дуги — операциям (маркерам) определения их достоверности (рис. 5).

Таблица 1

	1	**2**	**3**	**Vq**
1	5	4	3	**4**
2	6	10	2	**6**
3	7	8	1	**7**

Таблица 2

	1	**2**	**3**
1	∞	4	3
2	6	∞	2
3	7	∞	1

Таблица 3

	1	**2**	**3**
1	**10**	8	6
2	12	**20**	4
3	14	**16**	2

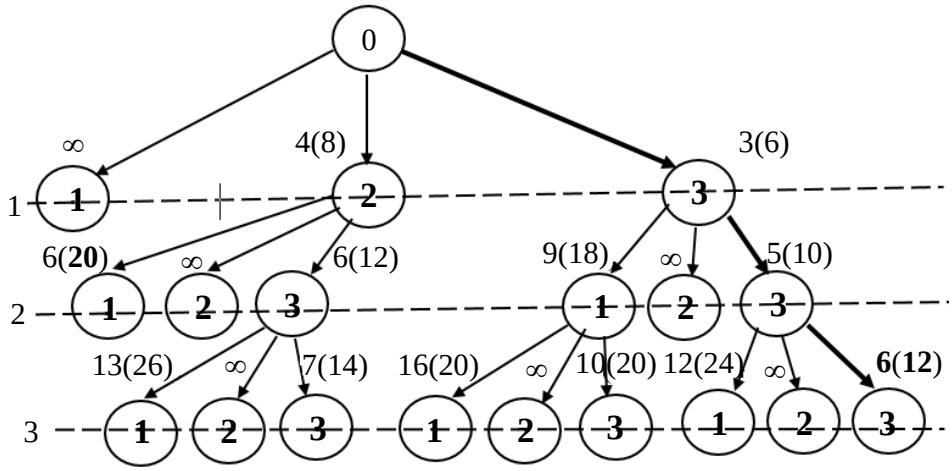


Рис. 4. Дерево решения (уровни дерева соответствуют номерам операций, а вершины на этих уровнях вариантам выбора маркера для этой операции)

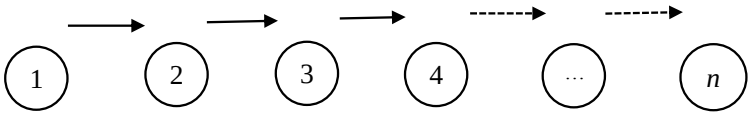


Рис. 5. Ориентированный линейный граф G (X, U)

Для анализа вариантов 1-го трейлера безопасности (ТБ) построим двойственный граф $G_1'(X_1', U_1')$, петли которого пересекают двойственные им дуги G (X, U) (рис. 6):

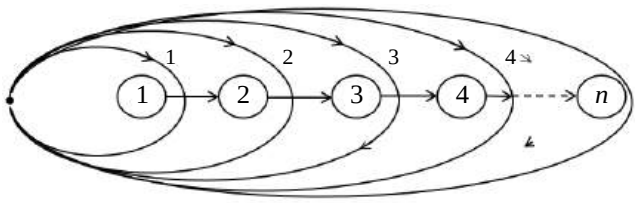


Рис. 6. Двойственный граф

Каждая петля (они выделены на рис. 6 штрихпунктирными линиями) соответствует одному ТБ, выполняющему операции, соответствующие дугам множества U, заключенными в одной петле.

Стягивая вершины множества X на G (X, U), ограниченные одной петлей, в одну вершину, получим новый граф, для которого справедливы все предшествующие преобразования. Таким образом будут выделены следующие комбинации объединения операций: операция 1 стягивается контурами {1,2}, {1,3}, {1,4}, …, {1, n}; операция 2 — конурами {2,3}, {2,4}, {1,4}, … {1, n}; операция 3 — контурами {3,4}, … , {1, n} и т. д.

Очевидно, что последовательность петель, таких, что (рис. 7):

1. Они охватывают все дуги графа G (X, U).

2. Вершина (i + 1)-й петли расположена "внутри" i-й петли (i = 1, 2, …) отвечает одному из возможных решений задачи.

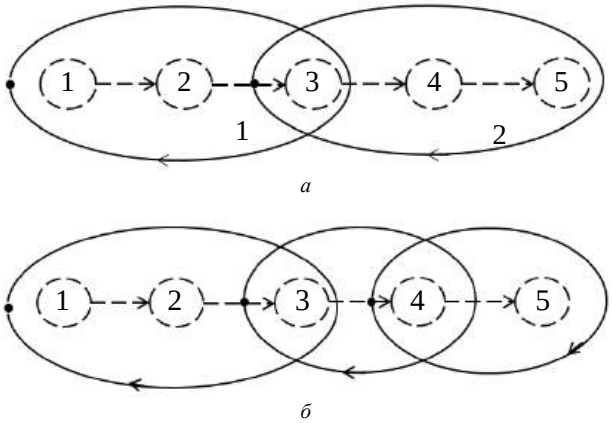


Рис. 7. Возможные варианты агрегирования трейлеров безопасности:
а — в 2 ТБ; *б* — в 3 ТБ

На рис. 7, *а* изображено преобразование, соответствующее объединению операций в 2 ТБ (1-й ТБ → {12}, 2-й ТБ → {34, 45}), а рис. 7, *б* — в 3 ТБ (1-й ТБ → {12, 23}, 2-й ТБ → {34}, 3-й ТБ → {45}).

Построим теперь новый граф $G_E(X_E, U_E)$, вершины которого совпадают с вершинами исходного линейного графа G (X, U), а каждой дуге $(ij) \in U_E$ отвечает одна из петель двойственного графа (рис. 8).

Легко убедиться, что для справедливы условия:

а) $|X_E| = |X|$; б) $|U_E| = ½\ |X_E|\ (|X_E| + 1)$;

в) $\forall j > i,\ (i, j) \in U_E$; г) граф G_E (X_E, U_E) не имеет контуров.

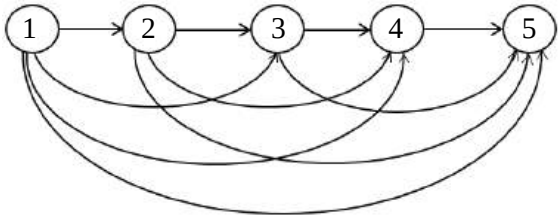


Рис. 8. Модифицированный граф $G_E(X_E,U_E)$

Присвоим каждой дуге $(ij) \in U_E$ два числа: $C(ij)$ стоимости установки на (ij)-й операции соответствующего ей маркера на доверенном оборудовании; $R(ij)$ — вероятности нарушения достоверности на операции $(ij) \in U_E$ (величина $R(ij)$ может быть получена методами экспертных оценок, математическим моделированием и т. п.). Булева переменная $x(ij)$ равна 1, если (ij)-й маркер включения ТБ и 0, в противном случае.

Формальная постановка задачи в этом случае имеет вид:

минимизировать суммарные затраты на формирование ТБ

$$\sum_{i=1}^{n} \sum_{j>i} C(i, j)\, x(i, j) \to \min \qquad (6)$$

при следующих ограничениях на:

непрерывность выполнения всех операций

$$\forall 1 < j < n : \sum_{i} x(i, j) = \sum_{k} x(j, k); \qquad (7)$$

выполнение всех операций иметь начальное состояние и конечное

$$\sum_{i=2}^{n} x(1, i) = \sum_{j>i}^{n-1} x(i, n) = 1; \qquad (8)$$

Максимальное значение вероятности нарушения достоверности на (ij) операции не должна меньше или равна заданному значению

$$\max_{(ij)\in U_E} R(i,j)x(i,j) \le P; \quad (9)$$

$$\forall(ij)\in U_E,\ x(i,j)=1,0 \quad (10)$$

где P — верхняя граница вероятности нарушения достоверности ТБ. Очевидно, что решению (6) на G_E (X_E, U_E) отвечает кратчайший путь из источника в сток, для каждой дуги которого $(i,j)\in U_E$ справедливо: $R(i,j)\le P$.

Алгоритмы решения задачи. Решение задачи (6)—(10) осуществляется в 2 этапа: на первом этапе на множестве U_E выделяется подмножество $U'_E \in U_E$, для которого справедливо: $\forall(ij)\in U_E; R(ij) > P$. На втором этапе на сети $G_E(X_E, U_E\backslash U'_E)$ каждой дуге которой $(ij) \in U_E\backslash U'_E$ присвоен вес $C(ij)$ ищется кратчайший путь из $x_1 \in X_E$ $x_n \in X_E$. Доказательство справедливости такого подхода тривиально.

Пример 3. Определить оптимальную стратегию агрегирования ТБ конвейерной обработки трех операций ЭлД, представленную на табл. 4. В таблице описаны петли двойственных графов, первое число соответствует весам $C(ij)$, второе — $R(ij)$. Величина $P \le 0{,}6$.

Таблица 4

	1	2	3	4
1	0; 0,0	2; 0,5	3; 0,6	9; 0,85
2		0; 0,0	2; 0,3	4; 0,9
3			0; 0,0	1; 0,4
4				0; 0,0

Соответствующий граф G_E (X_E, U_E) изображен на рис. 9:

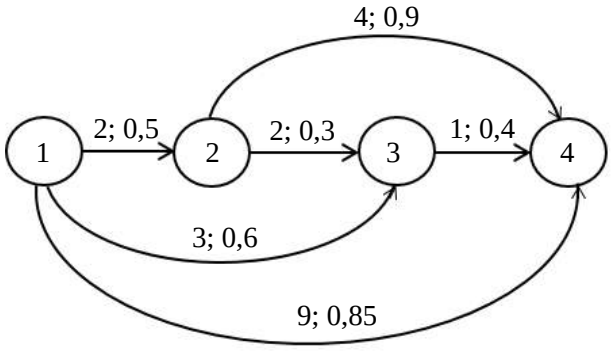


Рис. 9. граф G_E (X_E, U_E)

Дуги, входящие в U'_E = {(1,4); (2,4)}. Граф $G_E(X_E, U_E\backslash U'_E)$ изображен на рис. 10. Вес дуги $(ij) \in U_E\backslash U'_E$ равен $C(ij)$:

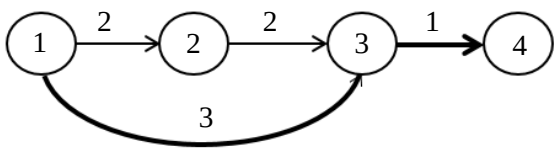


Рис. 10. Граф $G_E(X_E, U_E\backslash U'_E)$

Дуги кратчайшего пути выделены на графе (рис. 8) жирными линиями. Агрегированию соответствуют два ТБ: 1-й ТБ {1,2; 2,3} и 2-й ТБ {3,4}.

Заключение

Показано, что информационная технология обработки ЭлД, понимаемая как последовательность операций над данными, является предметом защиты. По аналогии с реальным миром для контроля целостности информационных технологий изготовления информационных документов в процессе информационного производства предложен механизм трейлеров безопасности. Рассмотрены условия эквивалентности информационных технологий. Приведен один из вариантов решения задачи выбора маркеров и их агрегирование для случаев распределенных информационных систем, в которых лишь часть является доверенной.

Литература

1. *Brodskiy A. V., Gorbachev V. A., Karpov O. E., Konyavsky V. A., Kuznetsov N. A., Raigorodskii A. M., Trenin S. A.* Identification in digital economy computer systems // J. Communications Technology and Electronics. 2019. V. 64. № 12. P. 1493—1499.

2. *Конявский В. А.* Доверенные системы как средство противодействия киберугрозам. Базовые понятия // Информационная безопасность. 2016. № 3. С. 40—41.

3. *Konyavsky V. A., Ross G. V.* Computer with changeable architecture // J. Mechanical Engineering Research and Developments. 2019. V. 42. № 3. P. 19—23.

4. *Конявский В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией. Серия "Библиотека журнала "УЗИ". — Минск, 2004. — 327 с.

5. *Конявский В. А.* Методы и аппаратные средства защиты информационных технологий электронного документооборота. Дисс. … докт. техн. наук. — М., 2005. — 360 с.

6. *Конявский В. А.* Информационные технологии как объект защиты и классификация антивирусных программ // Безопасность сетей и средств связи. 2007. Вып. 2. С. 52—54.

7. *Колмогоров А. Н.* Три подхода к определению понятия "Количество информации" // Новое в жизни, науке, технике. Сер. "Математика, кибернетика". 1991. № 1. С. 24—29.

8. *Трахтенброт Б. А.* Алгоритмы и вычислительные автоматы. — М., 1974. — 200 с.

9. *Росс Г. В.* Моделирование производственных и социально-экономических систем с использованием аппарата комбинаторной математики. — М.: Мир, 2001. — 304 с.

10. *Голубев-Новожилов Ю. С., Гроппен В. О., Росс Г. В.* Некоторые модели функционирования локальных вычислительных сетей на базе микро-ЭВМ // Электронная техника. Сер. 9. 1985. Вып. 3(56).

11. *Росс Г. В.* Математические модели формирования типового программного обеспечения для ЭВМ // Электронная техника. Сер. 9. 1988. Вып. 3(68).

Secure Information Technologies in the Digital Economy

V. A. Konyavsky
Moscow Institute of Physics and Technology (State University), Dolgoprudny, Moscow region, Russia

V. V. Medvedev
Russian New University, Moscow, Russia

G. V. Ross
Plekhanov Russian University of Economics, Moscow, Russia

Open information systems are being actively introduced into life, the relevance of protection in such systems is growing, but at the same time, the vast majority of approaches are focused only on corporate systems. The article discusses the features of information protection in open systems, characteristic of the digital economy. It is shown that it is necessary to take into account the requirements for the protection of information technologies, considered as a sequence of operations. For this purpose, a mechanism of security trailers is proposed, conditions for the equivalence of information technologies are considered. The problem of choosing markers and their aggregation is solved for cases of distributed information systems, including untrusted subsystems.

Keywords: information technology, digital economy, secure information technology, graph.

Bibliography — 11 references. *Received June 15, 2022*

УДК 004.056.52
DOI: 10.52190/2073-2600_2022_2_45
EDN: KRYLPB

Обеспечение информационной безопасности с помощью разведки по открытым источникам (OSINT)

В. И. Шармаев
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Я. А. Андреева; К. А. Василевский
ФГБОУ ВО Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации Ордена Трудового Красного Знамени «Московский технический университет связи и информатики», Москва, Россия

Выявлены особенности обеспечения информационной безопасности организации с помощью средств OSINT. Проанализированы сведения о компании, которые были обнаружены с помощью разведки по открытым источникам, выделены преимущества используемой методики. Особое внимание уделено анализу применяемых технологий и сетевых решениях, сведения о которых позволили выделить возможные риски, например, возможность атаки "межсайтового скриптинга" посредством уязвимостей jQuery или возможность определения списка действительных учетных записей с использованием уязвимостей WordPress. Результаты данного исследования можно использовать в разработке тактических и стратегических рекомендаций организациям по формированию более надежных политик информационной безопасности, выявлению уязвимостей и снижению рисков.

Ключевые слова: OSINT, разведка по открытым источникам, информационная безопасность, уязвимости, кибератаки, ИТ-инфраструктура.

Обширные инфраструктуры современных компаний включают множество сетей, устройств, технологий, а информация размещается на различных устройствах — компьютерах сотрудников, локальных серверах, удаленных серверах, на личных устройствах сотрудников. Это усугубляется тем фактом, что большинство компаний создают аккаунты в социальных сетях, где и хранится зачастую чувствительная информация.

В современном мире веб-сайты и социальные сети стали настоящими хранилищами личной информации сотрудников и сведений об ИТ-инфраструктуре компаний. Такие сведения могут быть использованы как для выявления потенциальных уязвимостей, так и для планирования кибератак. Именно здесь возникает поколение средств разведки по открытым источникам (англ. Open source intelligence, OSINT), которые подразумевают использование сбор, фильтрацию и анализ любых данных, предоставляемых открытыми источниками [1]. Основными функциями инструментов OSINT является поиск общедоступных активов и содержащихся в них информации и поиск информации за пределами компании. Такой поиск осуществляется, например, на собственных поддоменах сервисов организации или на доменах социальных сетей и других компаний, что характерно для крупных организаций. Успешность результатов такого анализа зависит от используемого в компании программного обеспечения и от квалификации сотрудников на критических должностях.

OSINT может применяться в различных сценариях [2]. Государственные структуры и ведомства используют его для обеспечения национальной безопасности и борьбы с терроризмом. Средства массовой информации таким способом определяют взгляды общественности по различным вопросам и для получения оперативных сведений о различных событиях. Международные организации используют OSINT-средства для межгосударственного взаимодействия, гуманитарные организации — для оказания помощи в кризисных ситуациях. Частные же компании используют разведку по открытым источникам для исследования рынка,

Шармаев Вадим Игоревич, магистрант.
E-mail: vadidq@ya.ru
Андреева Яна Андреевна, студентка.
E-mail: andreevaya.00@mail.ru
Василевский Кирилл Антонович, магистрант.
E-mail: alaxtver@yandex.ru

Статья поступила в редакцию 4 апреля 2022 г.

мониторинга деятельности конкурентов, для определения стратегий развития. Обычный пользователь сети Интернет, осознающий важность конфиденциальности, также может прибегать к инструментам OSINT, например, чтобы узнать, что другие пользователи могут узнать о них. Но используют OSINT и злоумышленники, определяя уязвимые места своих жертв, поэтому общим же для всех случаях является возможность использования OSINT для борьбы с утечками данных и анализа угроз как извне, так и изнутри организации. Эффективная политика управления рисками информационной безопасности позволяет обеспечить защиту интересов компании, ее репутации. Осознавая уровень уязвимости, можно закрыть пробел в безопасности и удалить чувствительные сведения, которые оказались в общественном доступе.

Наибольший интерес представляют корпоративные почтовые адреса, субдомены, используемые IP-адреса, конфиденциальные документы, открытые порты, используемые технологии и ПО, скрытые директории сайтов и конфиденциальные документы. Обнаруженные сведения могут помочь выявить уязвимые места, определить предполагаемый вектор атаки и, как следствие, выстроить систему безопасности так, чтобы не допустить ее.

Инструменты OSINT (то есть инструменты, использующиеся для сбора информации из общедоступных ресурсов и использования ее для принятия решений), могут использоваться как в злонамеренных целях, так и в целях противодействия им. Такой поиск информации является абсолютно законным, кроме тех случаев, когда собираемые данные защищены паролем или другим способом обеспечения конфиденциальности информации. На практике инструменты OSINT проверяют "открытые", то есть общедоступные для любого пользователя сети Интернет-ресурсы.

Инструменты OSINT помогают специалистам по информационной безопасности:

- собирать сведения для принятия решений;
- структурировать собранные сведения (например, в виде графиков, диаграмм);
- фильтровать сведения, используя различные ограничения;
- извлекать из собранных сведений полезную информацию.

Основной целью специалиста по информационной безопасности является поиск информации, представляющей риск для безопасности компании, и уменьшение последствий возможных атак злоумышленника, который могут воспользоваться этой информацией в своих целях. Для обнаружения слабых мест специалистами регулярно проводится тестирование. Конфиденциальные данные могут содержаться, например, в метаданных опубликованных в открытом доступе файлов. Помимо этого, источниками данных могут являться источники поставщиков и партнеров, социальные сети, глубоко проиндексированные веб-сайты компании, которые стали технически общедоступны. Поскольку информация является общедоступной, любой пользователь может получить доступ к ней, включая злоумышленников.

Специалист по информационной безопасности изначально должен определить, с какой целью он намерен использовать инструменты OSINT — как часть выявления слабых мест ИТ-инфраструктуры и уязвимостей ПО или как средство для определения информации, которую распространяют сотрудники в сети. В зависимости от этого определяется список инструментов, которые используются для дальнейшего сбора сведений и их анализа.

Теоретическая часть

Для поиска личной информации о сотрудниках и их работе используются социальные сети. В социальных сетях содержатся даты рождения, имена членов семьи, клички домашних животных, что может как содержаться в паролях пользователей, так и использоваться для фишинговых атак. Для обнаружения учетных записей и утечек информации злоумышленниками используются такие сервисы, как GitHub. Зачастую в коде встречаются ключи шифрования или даже пароли администраторов, либо информация об открытых портах, используемых в настройках облачных хранилищ.

Чувствительными сведениями об ИТ-инфраструктуре являются сведения об открытых портах и небезопасно подключенных устройствах; сведения об установленном программном обеспечении и его версии; имена устройств, сети и IP-адреса; утекшая информация (например, исходный код) [3].

Можно выделить три способа OSINT-разведки [4]:

- пассивный сбор информации — подразумевает сбор информации только через общедоступные ресурсы;
- полупассивный сбор информации — подразумевает отправку трафика на целевые серверы для получения информации о них без проведения углубленного расследования. Используемый трафик напоминает обычный интернет-трафик, чтобы не привлекать внимания средств защиты сети;

- активный сбор информации — подразумевает прямое взаимодействие с исследуемой системой, что позволяет получить детальные сведения, такие как открытые порты, наличие уязвимостей (например, использование нелицензионного или устаревшего ПО) и т. д. Такой трафик оставляет следы в системах защиты сетей.

Сканирование OSINT могут обнаружить десятки тысяч результатов, особенно в компании с обширной ИТ-инфраструктурой и в случае сканирования не только внутренних, но и внешних источников. Работать с таким количеством информации вручную затруднительно, поэтому зачастую специалисты используют готовые инструменты с открытым кодом, которые способны структурировать обнаруженную информацию для ее анализа. Среди наиболее известных инструментов [5]:

Сервис Maltego — предназначен для выявления связей между пользователями, компаниями, доменами и открытой информацией в сети Интернет [6]. Maltego визуализирует полученную информацию в виде диаграмм и графиков и связывает их источники (адреса электронной почты, компании, веб-сайты и т. д.).

Сервис WhatWeb — позволяет определить, какие технологии использует веб-сайт [7]. Сервис распознать системы управления контентом (CMS), библиотеки JavaScript, номера версий, идентификаторы учетных записей, ошибки SQL и другое.

Сервис Shodan — используется для обнаружения открытых портов в системе, подключенных устройствах, диапазоны IP-адресов, сетевую репутацию (размещалось ли вредоносное ПО и как быстро проблема была решена), при этом сохраняется исторические данные с разбивкой по месяцам и имеется возможность уведомлений в режиме реального времени [8].

Сервис Metagoofil — предназначен для загрузки с целевого сайта всех документов указанных типов, что в сочетании с утилитой exiftool позволяет извлечь метаданные из общедоступных файлов любых расширений [9]. Метаданные могут раскрыть имена пользователей, адреса электронных почт, используемое программное обеспечение и его версия, пути к файлам, электронные адреса. Сами по себе документы также могут содержать конфиденциальные сведения, не предназначенные для публикации в открытом доступе.

Сервис Searchcode — используется для просмотра исходного кода различного программного обеспечения, находящегося в открытом доступе [10]. С помощью него можно обнаружить, например, указанные в коде учетные записи пользователей, специальные символы, которые могут использоваться для атак с внедрением кода, а также уязвимости в системе безопасности. Похожий сервис, осуществляющий поиск по исходному коду, содержащемуся в репозиториях Git — Grep.app.

Сервис SpiderFoot — интегрирует в себе почти все доступные источники данных OSINT (например, AlienVault, HaveIBeenPwned, SecurityTrails и Shodan), подходит для обнаружения таких сведений, как IP-адреса, адреса подсетей, поддомены, email-адреса, номера телефонов, логины, а также визуализирует собранную информацию в виде таблиц и графиков [11].

Сервис Spyse — предназначен для сбора заголовков HTTP, robots.txt и обнаружения рисков безопасности на веб-сайтах и связанных серверах и устройствах [12]. Способен также обнаружить информацию об интернет-провайдере, геолокации, CHAME-записи и используемую версию SSL/TLS.

Сервис Intelligence X — архивная служба, которая сохраняет утечки данных с возможность поискового запроса среди этих данных, например, по адресу электронной почты, URL-адресу, IP-адресу [13].

Помимо перечисленных инструментов, существует множество других, используемых для разведки по открытым источникам. Полезным сервисом является платформа OSINT, представляющая собой фреймворк с ссылками на другие источники, которые можно использовать для сбора необходимой информации. Полезная информация также может быть найдена в архивах Интернета — сохраненных страницах, где может содержаться прежняя информация о сотрудниках, телефонные номера, адреса электронной почты, извлеченные из архивной версии целевого сервиса. Самым популярным таким архивом является Wayback Machine (https://archive.org/web/) [14].

Методология

В качестве демонстрации подхода к поиску уязвимостей с помощью разведки по открытым источникам был исследован веб-сайт консалтинговой компании D. — фирмы по поиску руководителей, расположенной в Кливленде, штат Огайо.

С помощью сервиса Maltego сформирован граф, вершинами которого являются различные сведения, найденные в открытых источниках (рис. 1).

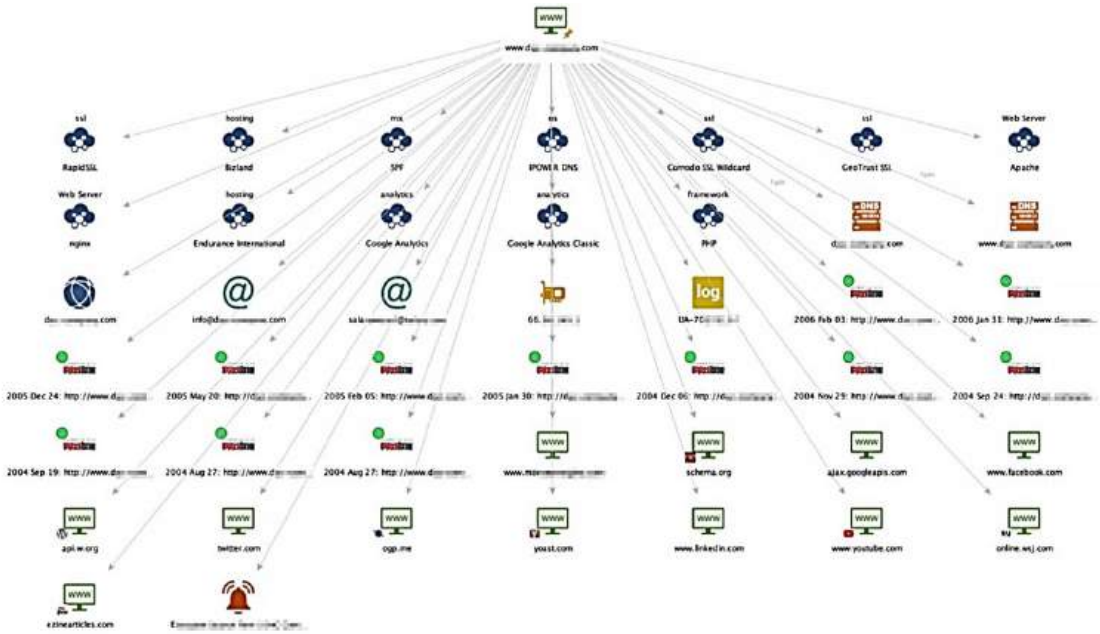


Рис. 1. Результат работы сервиса Maltego

В сформированном сервисом отчете содержится информация о DNS, IP-адресе сервера, найденные email-адреса, ссылки на сохраненные версии сайта сервиса Wayback Machine, а также используемые на сайте сторонние сервисы (ajax.googleapis.com, api.w.org, twitter.com, facebook.com, linkedin.com и другие) и технологии (Apache, Bizland, Comodo SSL Wildcard, IPOWER DNS, PHP, RapidSSL, SPF, nginx и другие).

Архивные копии сайта на сервисе Wayback Machine позволили обнаружить номера телефонов, указанные как контактные, но отсутствующие в текущей версии сайта.

Анализ метаданных документов, обнаруженных с помощью сервиса metagoofil, позволил узнать сведения об используемом оборудовании (Mac OS X 10.4.11), а также используемое (Adobe Photoshop CS6 Macintosh). Документы, обнаруженные сервисом metagoofil представлены на рис. 2.

С помощью сервиса Spyse собраны дополнительные сведения о дате регистрации сайта и его регистраторе, адреса серверов, а также информация об используемых на сайте технологиях (Apache, jQuery, Yoast SEO, Google Analytics, PHP, WordPress). Результат работы сервиса Spyse представлены на рис. 3.

Рис. 2. Документы, обнаруженные сервисом metagoofil

Рис. 3. Результат работы сервиса Spyse

Дополнительно проведено сканирование веб-сайта с помощью сервисов WhatWeb и SpiderFoot, которые подтвердили обнаруженные сведения.

Обсуждение

Собранные в открытых источниках данные могут использоваться злоумышленником для реализации кибератаки.

По указанному на сайте почтовому адресу удалось обнаружить список работников компании, их личные электронные почты и адреса, а также пароли, указанные на различных сайтах при регистрации с этим адресом (рис. 4). Такая информация является критичной, необходима регулярная проверка, а в случае обнаружения факта утечки данных — немедленная смена паролей всех сотрудников. Оправданной мерой является и запрет на регистрацию на сторонних сервисах с использованием корпоративного электронного адреса.

Рис. 4. Результат поиска сервиса Intelligence X

Рекламные идентификаторы сайта позволяют увидеть подробную статистику сайта, если она не была скрыта администратором — узнать количество посетителей сайта, распределение по странам и возрастам.

Открытых данных оказалось достаточно, чтобы обнаружить используемый на сайте SSL-сертификат с истекшим сроком годности. SSL-сертификат — это гарантия безопасности для пользователей веб-ресурса, без него злоумышленники могут похитить конфиденциальные сведения, следовательно, сайт подвержен риску атак "человек в середине". Менее опасные, но существенные последствия SSL-сертификата с истекшим сроком годности, — понижение в поисковой выдаче, снижение доверия пользователей, негативное влияние на корпоративный бренд и репутацию [15].

Информация об используемых на сайте технологиях позволяет определить иные векторы атак, например:

- В PHP до 7.1.3 злоумышленник может вызвать отказ в обслуживании с потреблением ресурсов центрального процесса путем переменных большого размера.
- WordPress до 2.8.1 по-разному реагируют на неудачную попытку в систему в зависимости от того, существует ли учетная запись пользователя или нет, что позволяет злоумышленнику определить действительные логины пользователей.
- jQuery до версии 1.9.0 допускает атаку "межсайтовый скриптинг" (Cross-Site Scripting) с помощью метода загрузки. Метод загрузки не может распознать и удалить HTML-теги "<script>", что приводит к выполнению логики скрипта.

В частности, сервис Spyce отметил уровень опасности как "Серьезный".

Таким образом, с помощью различных средств OSINT была собрана информация об используемом программном обеспечении, применяемых технологиях, сотрудниках, используемых паролях. На основании используемых технологий определены векторы атаки и их возможные последствия.

Заключение

Не каждая атака злоумышленника производится с помощью специализированного программного обеспечения. Злоумышленник, как и любой человек, всегда выбирает самый легкий путь к своей цели. Нет необходимости в течение нескольких месяцев искать уязвимые места ИТ-инфраструктуры компании, если нужные сведения содержатся в открытом доступе.

Используя традиционные инструменты, тяжело анализировать такой объем информации, который тем больше, чем больше сама компания. Инструменты OSINT позволяют структурировать эту информацию, упростить ее анализ. Простой поиск на одном из сайтов позволяет выявить сведения о критических объектах системы безопасности и подключенных в сеть устройствах. Разведка по открытым источникам становится все более важной частью системы информационной безопасности, а грамотное использование ее инструментов значительно улучшает процесс управления рисками.

Можно выделить ряд преимуществ методики сбора информации OSINT. Анализируемые источники находятся в открытом доступе, при этом можно легко их фильтровать или задавать дополнительные критерии. Использование таких средств делает работу управляемой — без дополнительных затрат в любой момент времени можно обнаружить потенциальные угрозы, при этом анализируемая информация представлена в удобном, структурированном виде. Как правило, использование инструментов OSINT значительно дешевле по сравнению с другими способами сбора информации как с точки зрения человеческих ресурсов,

так и с точки зрения стоимости программного обеспечения. Ресурсы OSINT могут использоваться без нарушения лицензий или авторских прав, так как анализируются исключительно открытые источники [16].

Компаниям необходимо противодействовать кибератакам с помощью грамотной оценки рисков. Использование инструментов OSINT позволяет обнаружить уязвимости и улучшить систему защиты организации, определив актуальные угрозы. OSINT позволяет найти сведения о компании, ее сетях, данных и пользователях. Такими сведениями могут быть поддомены, на которых размещены незащищенные конфиденциальные файлы, адреса портов, метаданные файлов, адреса веб-почт, номера телефонов и т. д. Ключевым моментом является скорость обнаружения этой информации, которую необходимо до того, как злоумышленник успеет воспользоваться ей.

Для специалистов в области информационной безопасности понимание того, как собирать и анализировать данные из открытых источников, является необходимым навыком. Независимо от того, разрабатывается ли система защиты или производится ее тестирование на наличие слабых мест, чем больше будет получено информации, тем лучше будет видна ИТ-инфраструктура с точки зрения злоумышленника.

Литература

1. *Минченко В., Вильдяйкин Г. Ф.* разведка на основе открытых источников (OSINT) и ее методология в современных реалиях // Молодежь и наука: актуальные проблемы фундаментальных и прикладных исследований. 2020. С. 319—322.
2. *Гурулев Д. А.* Бизнес-разведка на основе открытых источников с помощью автоматизированной информационной системы // Информационные технологии в науке, бизнесе и образовании. 2020. С. 56—61.
3. *Смирнов Д. В.* О возможностях анализа защищенности информационной системы организации на основе открытых источников информации // Межвузовская научно-техническая конференция студентов, аспирантов и молодых специалистов им. Е. В. Арменского. 2019. С. 213—214.
4. *Басыня Е. А., Хищенко В. Е., Рудковский А. А.* Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации // Доклады ТУСУР. 2019. № 2. С. 6—7.
5. Инструментов разведки с открытым исходным кодом: SecurytiLab. [Электронный ресурс]. 2021. Дата обновления: 27.04.2021. URL: https://www.securitylab.ru/blog/company/CABIS/350642.php (дата обращения: 08.04.2022).
6. Сервис maltego. [Электронный ресурс]. Режим доступа: https://www.maltego.com/.
7. Сервис WhatWeb. [Электронный ресурс]. Режим доступа: https://github.com/urbanadventurer/WhatWeb.
8. Сервис shodan. [Электронный ресурс]. Режим доступа: https://www.shodan.io/.
9. Сервис metagoofil. [Электронный ресурс]. Режим доступа: https://code.google.com/archive/p/metagoofil/.
10. Сервис searchcode. [Электронный ресурс]. Режим доступа: https://searchcode.com/.
11. Сервис spiderfoot. [Электронный ресурс]. Режим доступа: https://www.spiderfoot.net/.
12. Сервис spyse. [Электронный ресурс]. Режим доступа: https://spyse.com.
13. Сервис intelx. [Электронный ресурс]. Режим доступа: https://intelx.io/.
14. Сервис archive. [Электронный ресурс]. Режим доступа: https://archive.org/web/.
15. *Каликулина З. В.* Анализ основных уязвимостей веб-приложений // Ответственный редактор. 2019. С. 46.
16. *Додонов А. Г., Ландэ Д. В., Прищепа В. В., Путятин В. Г.* Компьютерная конкурентная разведка // ТОВ Инжиниринг. 2021. С. 113—115.

Information security through open source intelligence (OSINT)

V. I. Sharmaev
Moscow Aviation Institute (National Research University), Moscow, Russia

Ya. A. Andreeva, K. A. Vasilevsky
Moscow Technical University of Communications and Informatics, Moscow, Russia

The aim of the study is to identification of any unusual features of organization using OSINT. In order to achieve the goal was analysed the information about company, which was detected with technology of OSINT, also noted advantages of using method. A special emphasis on analysis of used technologies and network solutions, this information allowed identify potential risks such as 'cross-site scripting' through vulnerability of jQuery or allowed definition of current account's list through vulnerability of WordPress. The results of the research could be used in development of tactical and strategic recommendations to the organizations that could be develop more reliable security policy, detect vulnerabilities and reduct any risks.

Keywords: OSINT, open source intelligence, information security, vulnerabilities, cyberattacks, IT infrastructure.

Bibliography — 16 references. *Received April 4, 2022*

УДК 004.056.5
DOI: 10.52190/2073-2600_2022_2_51
EDN: KYSIHX

Использование метода экспертных оценок при определении уровня защищенности информационной системы

Д. В. Титов, канд. техн. наук; *Е. Е. Филипова*, канд. физ.-мат. наук
ФКОУ «Вологодский институт права и экономики ФСИН России», г. Вологда, Россия

Рассмотрен способ применения метода экспертных оценок в качестве инструмента для анализа информационной системы по различным направлениям защиты информации.

Ключевые слова: экспертная оценка, информационная система, уровень информационной безопасности, аудит, коэффициент конкордации.

В процессе функционирования информационных систем в организациях могут возникать ситуации, при которых наступает неопределенность в действиях персонала по обеспечению сохранности данных, валидности применяемых паролей и неоднозначного подхода к самому процессу защиты информации.

В информационной системе при несогласованности в действиях персонала и специалистов по защите информации может снижаться уровень информационной безопасности. В этом случае вероятность "кибератак" и вторжений резко возрастает, риски угроз информационной безопасности могут превышать допустимые значения.

При значительных потерях данных, очевидно, встанет вопрос о качестве и значимости принимаемых организационных и технических мер по обеспечению защиты. На практике зачастую руководствуются средствами устранения недостатков "по месту", анализируя лишь конкретные рабочие места и информацию, доступную пользователям, при этом у специалистов затрачивается время на устранение причин сбоев, а также работы, связанные с резервным копированием, переносом баз данных, исправлением ошибок в операционных системах, устранением технических утечек информации и т. п. Таким образом, в реальном времени, система все еще остается уязвимой для возможных атак извне.

Титов Дмитрий Валерьевич, доцент кафедры "Информатика и математика" факультета психологии и права.
E-mail: titov_dv@mail.ru
Филипова Елена Евгеньевна, доцент кафедры "Информатика и математика" инженерно-экономического факультета.
E-mail: lenphil@mail.ru

Статья поступила в редакцию 17 мая 2022 г.

Поэтому, на наш взгляд, целесообразно построить прогнозируемую систему информационной безопасности для противостояния киберугрозам, основанную на использовании опытных оценок с помощью всестороннего аудита безопасности. Данный метод не требует значительных затрат и позволяет оценивать и анализировать состояние защиты системы по известным аспектам безопасности: доступность, целостность и конфиденциальность.

В качестве субъекта оценивания можно задействовать экспертов, имеющих беспристрастный подход к определению качественных характеристик мер по защите информации, применяемых в данной организации или учреждении.

Практическое значение подобных экспертиз обусловлено независимой оценкой каждым экспертом состояния защиты информационной системы по определенным направлениям.

Известно, что достоверность полученных результатов зависит от компетентности экспертов и их количества. Предположим, что все эксперты имеют достаточный уровень профессионализма, тогда можем утверждать, что с увеличением их числа достоверность результатов будет приемлемой. Для определения согласованности мнений специалистов необходимо рассчитать дисперсионный коэффициент конкордации [1] и оценить его значимость с помощью критерия χ^2 Пирсона. Чем ближе коэффициент конкордации к 0, тем меньше согласованность между экспертами [1, 2].

Рассмотрим пример анализа системы защиты метода на примере организации с помощью независимых экспертных оценок. В табл. 1 представлены оценки экспертов четырех направлений защиты, выставляемых по 5-балльной шкале.

Таблица 1

Оценки экспертов четырех направлений защиты, выставляемых по 5-балльной шкале

Номер эксперта	Характеристики оценивания			
	Уровень защиты файлов электронных документов на физических носителях	Уровень разграничения доступа к данным (конфидент)	Целостность баз данных, в том числе, на удаленных серверах	Доступность внутренних сервисов информационной системы
Эксперт 1	2	5	4	3
Эксперт 2	1	3	1	2
Эксперт 3	4	4	5	2
Эксперт 4	5	2	4	1
Эксперт 5	5	3	2	3
Сумма оценок	17	17	16	11

Матрица

$$R=\left(r_{ij}\right)=\begin{pmatrix}2&5&4&3\\1&3&1&2\\4&4&5&2\\5&2&4&1\\5&3&2&3\end{pmatrix},\ \left(i=1,\dots,5,\ j=1,\dots,4\right) \qquad (1)$$

представляет собой совокупность оценок i-го эксперта для j-й характеристики.

Коэффициент конкордации W в случае связанных рангов (наличии одинаковых оценок у одного и того же эксперта) рассчитывается по формуле:

$$W=\frac{12\,S}{m^2(n^3-n)-m\sum\limits_{i=1}^{m}T_i}, \qquad (2)$$

где m — количество экспертов (m = 5);

n — количество оцениваемых характеристик (n = 4),

$$S=\sum_{j=1}^{n}\left(\sum_{i=1}^{m}r_{ij}-\overline{r}\right)^2, \qquad (3)$$

$\sum\limits_{i=1}^{m}r_{ij}$ — сумма оценок для каждой характеристики (j = 1, …, n),

$\overline{r}=\dfrac{\sum\limits_{j=1}^{n}\sum\limits_{i=1}^{m}r_{ij}}{n}=\dfrac{61}{4}=15,25$ — среднее арифметическое суммарных оценок характеристик,

$T_i=\sum\limits_{k=1}^{H_i}\left(h_k^3-h\right)$ — показатель связанных рангов (одинаковых оценок эксперта).

Выполним расчеты связанных рангов и сформируем табл. 2.

Таблица 2

Эксперт	Количество групп связанных рангов, H	Количество связанных рангов в группе, h	T_i — показатель связанных рангов
1	0	0	$T_1 = 0$
2	1	2	$T_1 = 2^3 - 2 = 6$
3	1	2	$T_3 = 2^3 - 2 = 6$
4	0	0	$T_4 = 0$
5	0	0	$T_5 = 0$
			$\Sigma T_i = 12$

Подставляя данные в формулу (3), получим:

$$S=\sum_{j=1}^{n}\left(\sum_{i=1}^{m}r_{ij}-\overline{r}\right)^2=85,31.$$

Далее вычисляем собственно коэффициент конкордации по формуле (2):

$$W=\frac{12\cdot S}{m^2\cdot\left(n^3-n\right)-m\sum\limits_{i=1}^{m}T_i}=\frac{12\cdot 85,31}{5^2\cdot\left(4^3-4\right)-5\cdot 12}=0,72.$$

Оценим значимость коэффициента конкордации с помощью критерия χ^2 Пирсона по формуле

$$\chi^2=\frac{12\cdot S}{m\cdot n\cdot\left(n+1\right)-\dfrac{1}{n-1}\sum\limits_{i=1}^{m}T_i}=10,66.$$

Для уровня значимости α = 0,05 и числа степеней свободы $s = n - 1 = 3$ критическое значение критерия равно $\chi^2_{\text{крит.}}=7,8$. Если расчетное значение критерия оказалось больше критического, то гипотезу о согласии экспертов принимают.

Заключение

Данный способ в виде математической модели позволяет проанализировать уровень защищенности информационной системы, основываясь на независимых оценках различных направлений направлениям защиты информации. Аудит безопасности позволяет своевременно принимать решения, направленные на сохранение уровня информационной безопасности при возможных атак извне.

Литература

1. *Постников В. М., Спиридонов С. Б.* Подход к увеличению уровня согласованности мнений экспертов при выборе варианта развития системы обработки информации // Наука и образование. 2013. № 6. С. 333—350.
2. *Шмерлинг Д. С., Дубровский С. А., Аржанова Т. Д., Френкель А. А.* Экспертные оценки. Методы и применения (Обзор) // Уч. Зап. по Статистике, Т. 29. Статистические методы анализа экспертных оценок. — М.: Наука, 1977. С. 290—382.

Using the method of expert assessments when determining the security level of an information system

D. V. Titov, E. E. Filipova
Vologda Institute of Law and Economics of the Federal Penitentiary Service of Russia, Vologda, Russia

The method of applying the method of expert assessments as a tool for analyzing an information system in various areas of information protection is considered.

Keywords: peer review, information system, information security level, audit, concordance factor.

Bibliography — 2 references. *Received May 17, 2022*

БЛАНК-ЗАКАЗ НА ПОДПИСКУ 2022 г.
на издания ФГУП «НТЦ оборонного комплекса «Компас»

Наименование издания	Периодич-ность в год	Цена 1 экз., руб.	Кол-во выпусков в год	Общая сумма, руб.
Оборонный комплекс — научно-техническому прогрессу России	4	1550,00		
Конструкции из композиционных материалов	4	1700,00		
Экология промышленного производства	4	1500,00		
Информационные технологии в проектировании и производстве	4	1750,00		
Вопросы защиты информации	4	1750,00		
В цену включены: НДС — 10 % и стоимость почтовой доставки.				

Поставка журналов подписчикам через издательство осуществляется почтовыми бандеролями с приложением всех необходимых бухгалтерских документов.

Наши реквизиты:

Полное наименование организации: _____

Сокращенное наименование организации: _____

ИНН/КПП _____

ОКПО _____

Расчётный счёт № _____ в _____

к/с _____ БИК _____

Юридический адрес: _____

Почтовый адрес: _____

Контактное лицо _____ тел. _____

E-mail: _____

(Для оформления счёта и бухгалтерских документов просьба заполнить все строчки).

Справочно:
Заполненный бланк-заказ просьба отправить по факсу: 8(495) 491-44-80 или
E-mail: secretariat@ntckompas.ru
Более подробную информацию об изданиях и подписке можно получить по телефону:
8 (495) 491-43-17.
E-mail: ivleva@ntckompas.ru
Адрес редакции: 125424, Москва, Волоколамское шоссе, д.77.
ФГУП «НТЦ оборонного комплекса «Компас».

Правила для авторов по оформлению рукописей статей, предлагаемых к публикации в журналах

Направляя рукопись статьи в редакцию журнала, авторы передают редколлегии и издателю журнала безвозмездное неисключительное право опубликовать ее на русском языке в качестве статьи в печатной и электронной версиях журнала в сети Интернет. При этом за авторами сохраняются их интеллектуальные права на рукопись статьи (в том числе "авторское право"). В связи с этим и с учетом Четвертой части (Раздел VII) Гражданского кодекса РФ авторами должно быть представлено в редакцию письмо в следующей форме:

Лицензионный договор о передаче права на публикацию
(издательский лицензионный договор)

Мы, нижеподписавшиеся, авторы рукописи ……..……., предоставляем редколлегии журнала и журнала и издателю ФГУП «НТЦ оборонного комплекса «Компас» ……..……
(название журнала)
безвозмездную простую (неисключительную) лицензию на публикацию рукописи статьи как в печатной, так и в электронной версиях журнала.

Мы подтверждаем, что данная публикация не нарушает интеллектуальных прав других лиц или организаций.

Подписи авторов: …… (ф.и.о., ученая степень, дата)
……..…….
……...…….

Статья должна быть подписана всеми авторами. В случае нескольких авторов указывается фамилия автора, ответственного за переписку с редакцией. Рукопись статьи направляется на адрес редакции журнала: 125424, Москва, Волоколамское ш., д. 77, ФГУП «НТЦ оборонного комплекса «Компас», Редакция журнала. Дополнительная информация может быть получена в редакции при обращении по телефону: 8 (495) 491-43-17 или по E-mail: izdanie@ntckompas.ru.

Каждая статья рецензируется в соответствии с решением редколлегии журнала. Рецензенты выбираются из числа ученых и специалистов, компетентных в вопросах, рассматриваемых в статье, и имеющих собственные публикации в данном направлении. Решение о порядке публикации статьи принимается редколлегией с учетом мнения рецензентов. В случае разногласий среди членов редколлегии окончательное решение принимает главный редактор. При полном отклонении рукописи статьи от публикации редакция журнала направляет авторам мотивированный отказ. По этому факту редакция не вступает в полемику с авторами.

Комплектование статьи (обзора)

Статья должна быть представлена в редакцию в следующем комплекте:

- сопроводительное письмо, подписанное руководством организации;
- экспертное заключение о возможности опубликования в открытой печати и распространения в Российской Федерации и других государствах. При отсутствии в организации экспертной комиссии вместо экспертного заключения может быть представлено соответствующее заявление на имя главного редактора журнала от имени руководства организации, где работают авторы. В экспертном заключении или заявлении в обязательном порядке должна быть отражена возможность открытой публикации и передачи публикуемых материалов за границу.
- лицензионный договор по приведенному образцу;
- рукопись статьи — объем статьи (без рисунков) не должен превышать 10 страниц формата А4 при 1,5 межстрочных интервалах, а объем статьи обзорного характера — 20 страниц. Рекомендуемая гарнитура — New Times Roman. Размер шрифта — 12;
- Материал статьи представляется в редакцию в печатном виде (на бумажном носителе) и в электронном варианте с текстом в формате Word на электронную почту.

Оформление статьи:

- статья начинается с указания УДК;
- название статьи набирается строчными буквами (кроме начальной прописной) полужирным шрифтом, размер шрифта 14, для остального текста используется простой шрифт размером 12, причем рекомендуемая гарнитура шрифта — Times New Roman;
- после названия — список авторов, инициалы авторов предшествуют их фамилиям;

- далее представляется аннотация статьи (10—15 строк с раскрытием цели работы и её основных результатов);
- далее приводится список ключевых слов для данной статьи (не более десяти);
- страницы текста нумеруются без пропусков и добавлений литерных обозначений (типа 1*а*, 2*б* и т. п.), причем в сквозную нумерацию должны быть включены все элементы статьи;
- внизу первой страницы текста помещается отдельный абзац (с полужирным шрифтом), содержащий контактную информацию об авторе (или авторах) в следующем виде: фамилия, имя, отчество, должность, ученая степень, почтовый адрес предприятия, телефон, E-mail;
- основной текст статьи должен начинаться с четкой постановкой цели и задач работы, сопровождаемой аргументами в пользу ее выполнения на фоне существующего состояния затронутой в статье проблемы. Дальнейший текст статьи также должен иметь смысловые рубрикаторы (разделы и подразделы) без их нумерации. Заканчиваться статья должна отдельным разделом «Заключение» с перечислением основных результатов, следующих из них выводов и, по возможности, предложений по развитию исследований и использованию их результатов.
- после основного текста — список использованных источников "Литература" (не менее 5 источников); Список использованной литературы должен соответствовать всем ссылкам на внешние источники в тексте статьи. Ссылки оформляются в квадратных скобках, например, [1—6], [7, 8]. Внутренние ссылки, т. е. ссылки на формулы, рисунки и таблицы статьи оформляются с использованием круглых скобок, например, формула (1), уравнение (4), (рис. 3), (табл. 2). Любые ссылки в подписях к рисункам и в самих рисунках не рекомендуются;
- далее размещается подробная англоязычная информация о статье: название статьи, фамилия и инициалы авторов (английская транслитерация), предприятие, аннотация, ключевые слова (Keywords).

Оформление рисунков:

- рисунки и графики вставляются непосредственно в нужном месте в статье и в желаемом масштабе.
- рядом с осями графиков указываются отображаемые физические величины только в символьной (буквенной) форме, а через запятую — размерность величины по-русски (прямым шрифтом). Различные кривые на графиках рекомендуется нумеровать, даже если они характеризуются отдельным цветом или типом линии. Графики представляются только на белом фоне. Вспомогательные сетки на площади графика не допускаются;
- подписи под соответствующими рисунками (полужирный курсивный) представляются в нужных местах текста. Каждая подпись должна быть по возможности лаконичной, но емкой по содержанию.

Оформление формул:

- простые формулы вводить в текст в формате используемого текстового редактора, более сложные формулы — с использованием редактора формул MathType;
- стандартные математические обозначения (например, max, log, sin, exp и т. д.) должны быть набраны прямо. То же относится к цифрам и числам;
- для символьного обозначения невекторных физических (технических) величин использовать только латинский и греческий алфавиты, при этом в тексте для греческих букв использовать прямой шрифт, для латинских букв — наклонный шрифт (курсив);
- векторы и матрицы обозначать полужирным прямым шрифтом;
- для нижних и верхних индексов применять арабские цифры, латинские или греческие буквы. Если индекс представляет собой сокращенную форму русского слова — характеристики, то допустимо использовать в его обозначении русские буквы (прямой шрифт), например $U_{вх}$, $I_{вых}$, $\nu_{гр}$ и т. п.
- размерность физических величин обозначается всегда только по-русски прямым шрифтом.

Оформление таблицы:

- содержание таблицы не должно дублировать данные, приводимые на графиках или в тексте;
- графы должны иметь название без сокращения отдельных слов.

Рисунки, формулы и таблицы должны иметь свою отдельную сквозную нумерацию. Если на конкретную формулу нет дополнительных (возвратных) ссылок в тексте или она в единственном числе, то нумерация ее не нужна. Единственные таблица и/или рисунок также не нумеруются.

При публикации в журнале каждая статья (в контактной информации) сопровождается сноской со знаком охраны авторского права ©, поставленным перед фамилией автора (фамилиями авторов) и годом издания.

Авторы (или автор) каждой статьи после выхода журнала в свет имеют право на получение от редакции электронной версии статьи в PDF-формате (редактор Adobe Acrobat).