КРИПТОГРАФИЧЕСКИЙ РЕКУРСИВНЫЙ КОНТРОЛЬ ЦЕЛОСТНОСТИ МЕТАДАННЫХ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ. ЧАСТЬ 4. ОЦЕНКА ЗАЩИЩЕННОСТИ

Тали Д.И.[1], Финько О.А.[2]

Цель исследования *состоит в получении численной оценки результатов способа криптографического рекурсивного 2-D контроля целостности метаданных электронных документов.*

Методы исследования: *логико-вероятностный метод И.А. Рябинина.*

Результат исследования: *необходимым условием поддержания целостности электронных документов, обрабатываемых автоматизированными информационными системами электронного документооборота, является обеспечение требуемого уровня защищенности метаданных. Для оценки результатов исследования в качестве показателя эффективности выбрана вероятность нарушения целостности электронных документов.*

Представленный подход к построению логико-вероятностных моделей оценивания уровня защищенности метаданных электронных документов позволяет на практике получать численные значения вероятностей перехода рассматриваемых систем в опасное состояние (связанное с нарушением целостности метаданных электронных документов), с учетом структуры таких систем и реальных условий их функционирования.

Эффект от применения разработанного способа в условиях деструктивных воздействий уполномоченных пользователей (инсайдеров), по сравнению с известными решениями (применение хэш-функции) подобных задач, составляет 67 % при заданных допущениях.

Ключевые слова: *структурно-сложные системы, автоматизированные информационные системы, электронный документооборот, защищенность метаданных, алгебра логики, теория вероятности, функция опасного состояния системы, сценарий функционирования системы, хэш-функция.*

Статья завершает цикл тематических статей, начало которому было положено в пятом номере 2020 г. нашего журнала.

DOI: 10.21681/2311-3456-2021-2-37-50

Введение

Структурно-сложные системы, к числу которых относится АИС ЭД, имеют логико-вероятностную природу и, как следствие, могут быть описаны с использованием логико-вероятностных методов [1-6]. В этом случае предполагается, что структура АИС ЭД будет описываться средствами математической логики, а количественная оценка уровня защищенности производится с помощью теории вероятностей.

В основе логико-вероятностного метода (ЛВМ) лежат следующие положения [7]:

1) каждой логической операции соответствует функция, принимающая значения 1; 0, аргументы которой также принимают значения 1; 0. Такие функции называются функциями алгебры логики (ФАЛ);

2) элементы системы связаны логическими операциями конъюнкции, дизъюнкции и отрицания;

3) аналитическое описание опасного состояния осуществляется с помощью логической функции опасного состояния системы (ФОСС), аргументами которой выступают так называемые инициирующие события (воздействия) (ИнС, ИнВ), в качестве которых могут рассматриваться умышленные и неумышленные деструктивные воздействия уполномоченных пользователей АИС ЭД.

1 Тали Дмитрий Иосифович, адъюнкт 21 кафедры (тактико-специальной связи) Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: dimatali@mail.ru

2 Финько Олег Анатольевич, доктор технических наук, профессор, профессор 22 кафедры (техники специальной связи) Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, профессор кафедры информационной безопасности автоматизированных систем Северо-Кавказского федерального университета; академический советник Российской академии ракетных и артиллерийских наук (РАРАН), г. Краснодар, Россия. E-mail: ofinko@yandex.ru. Web: http://www.mathnet.ru/person40004.

ФОСС может быть получена или с помощью кратчайших путей опасного функционирования (КПОФ), или с помощью минимальных сечений предотвращения опасности (МСПО) [7]. Кратчайший путь опасного функционирования представляет собой такую конъюнкцию ИнС x_i, ни одну из компонент которых нельзя изъять, не нарушив опасного функционирования системы.

Такую конъюнкцию можно записать в виде ФАЛ:

$$\Phi_l = \bigwedge_{i \in K_{\Phi_l}} x_i \qquad (1)$$

где: K_{Φ_l} – множество номеров ИнС, соответствующих данному l-му КПОФ $\left(l \in N\right)$.

Инициирующее событие принимает одно из двух значений:

$$x_i = \begin{cases} 1, \text{ если } i\text{-е условие выполняется} \\ 0, \text{ если } i\text{-е условие не выполняется} \end{cases}$$

Иначе говоря, КПОФ описывает один из возможных самостоятельных вариантов перехода системы в опасное состояние с помощью минимального набора ИнС, необходимых для его осуществления.

МСПО представляет собой такую конъюнкцию из отрицаний ИнС x_i, ни одну из компонент которых нельзя изъять, не нарушив условия безопасного функционирования системы. Такую конъюнкцию можно записать в виде следующей ФАЛ:

$$\Psi_j = \bigwedge_{i \in K_{\Psi_j}} x_i^{'} \qquad (2)$$

где: K_{Ψ_j} – множество номеров, соответствующих данному j-му МСПО.

МСПО описывает один из возможных способов нарушения опасного функционирования с помощью минимального набора запрещенных условий. АИС ЭД имеет конечное число КПОФ $\left(l = 1,\ 2,\ \ldots,\ d\right)$ и МСПО $\left(j = 1,\ 2,\ \ldots,\ n\right)$. Используя эти понятия, можно поразному записать условия опасного состояния АИС ЭД:

в виде дизъюнкции всех имеющихся КПОФ:

$$f\left(x_1,\ \ldots,\ x_m\right) = y\left(x_m\right) = \bigvee_{l=1}^{d} \Phi_l = \bigvee_{l=1}^{d} \left(\bigwedge_{i \in K_{\Phi_l}} x_i \right); \qquad (3)$$

в виде конъюнкций отрицаний всех МСПО:

$$f\left(x_1,\ \ldots,\ x_m\right) = y\left(x_m\right) = \bigwedge_{j=1}^{n} \Phi_l^{'} = \bigwedge_{j=1}^{n} \left(\bigvee_{i \in K_{\Psi_j}} x_i \right). \qquad (4)$$

При этом ФОСС совокупности взаимодействующих АИС ЭД или выделенных из АИС ЭД совокупностей ее подсистем может быть представлена системой частных ФОСС. Кроме того, одна и та же ФОСС может рассматриваться не только в качестве самостоятельного объекта анализа, но и входить в систему ФОСС, описывающую более сложный сценарий функционирования системы (перехода АИС ЭД в опасное состояние) [8].

Оценка результатов исследования

В простейшем случае процесс функционирования АИС ЭД может быть описан следующей математической моделью [7]. В любой произвольный момент времени t, в процессе обработки ЭлД, подсистема защита информации (ЗИ) АИС ЭД может находиться в одном из двух состояний $S(t) = \left\langle S_{(+)}(t),\ S_{(-)}(t) \right\rangle$, по отношению к обрабатываемому j-му ЭлД $\left(D_j\right)$ при возникновении i-ого ИнС x_i в АИС ЭД (рис. 1):

$$S_{(+)}^{(x_i)}(t) : D_j \to 1, \qquad (5)$$

где: $S_{(+)}^{(x_i)}(t)$ – состояние ЭлД $\left(D_j\right)$, при котором в ходе реализации ИнС или ИнВ x_i целостность его метаданных не нарушена «1»;

$$S_{(-)}^{(x_i)}(t) : D_j \to 0, \qquad (6)$$

где: $S_{(-)}^{(x_i)}(t)$ – состояние ЭлД $\left(D_j\right)$, при котором в ходе реализации ИнС или ИнВ x_i целостность его метаданных нарушена «0».

Невозможность поддержания состояния $S_{(+)}^{(x_i)}(t)$ подсистемой ЗИ АИС ЭД следует рассматривать как событие, характеризующее переход АИС ЭД в опасный режим работы, проявляющийся в нарушении процесса управления ЭлД, сбое в работе, и как следствие, при продолжительном воздействии ИнС x_i, отказе в обслуживании [9-11].

В целях получения численной оценки результатов исследования произведем сравнение уровня защищенности метаданных ЭлД, обеспечиваемого за счет использования традиционной хеш-функции и разработанного технического решения, при умышленном и неумышленном нарушении целостности метаданных уполномоченными пользователями, а также при их совместном осуществлении. Для чего построим соответствующие сценарии перехода АИС ЭД в опасный режим работы (нарушение целостности метаданных ЭлД).

Рассмотрим сценарий реализации угрозы нарушения целостности метаданных ЭлД при использовании хеш-функции (рис. 2).

В качестве ИнС здесь выступают:

x_1 – несанкционированное изменение метаданных ЭлД администратором, использующим ключи $k_\varsigma^{(2)} \in \mathbf{K}_U^{(2)}$;

x_2 – несанкционированное изменение метаданных ЭлД оператором, использующим ключи $k_\varsigma^{(3)} \in \mathbf{K}_U^{(3)}$;

x_3 – компрометация внутренних ключей АИС ЭД $k_\varsigma^{(1)} \in \mathbf{K}_U^{(1)}$ / сбой в работе АИС ЭД;

x_4 – ошибка ввода метаданных ЭлД оператором;

x_5 – отсутствие контроля со стороны администратора.

Рассматриваемому сценарию будет соответствовать следующая ФАЛ, описывающая функцию перехода АИС ЭД в опасный режим работы:

$$f(x_1,\ \ldots, x_5) = (x_1 \vee x_2) \vee x_3 \vee (x_4 x_5). \qquad (7)$$

Составим ФОСС с помощью КПОФ:

$\Phi_1 = x_1 x_2,\ \Phi_2 = x_3,\ \Phi_3 = x_4 x_5.$

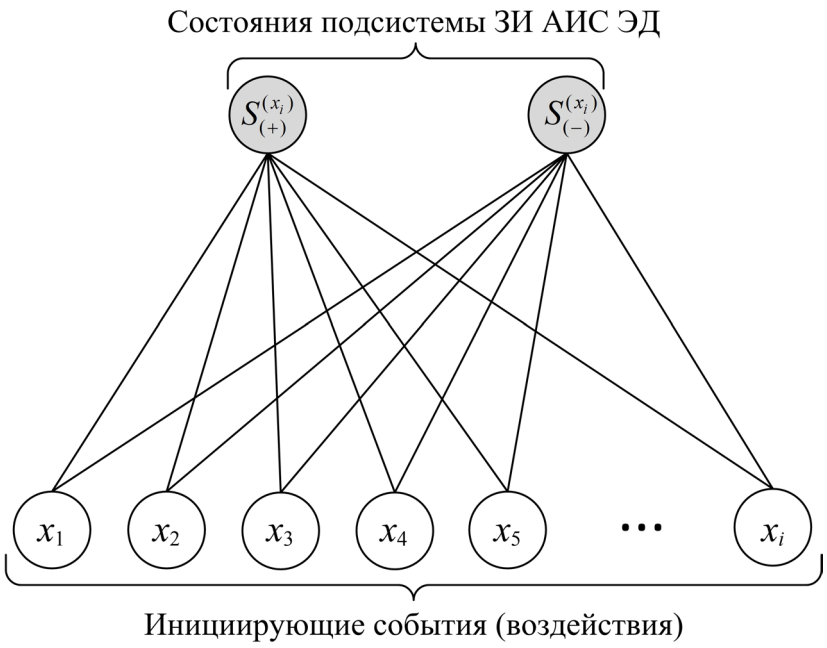

Рис. 1. Граф переходов подсистемы ЗИ АИС ЭД в состояния $S_{(+)}^{(x_i)}$ *и* $S_{(-)}^{(x_i)}$

В соответствии с ЛВМ [1] преобразуем полученную ФАЛ (7) в форму перехода к полному замещению (ФППЗ), допускающую замену логических переменных соответствующими вероятностями. В настоящее время известно несколько ФППЗ: совершенная дизъюнктивная нормальная форма (СДНФ), ортогональная дизъюнктивная нормальная форма (ОДНФ) и бесповторные ФАЛ в базисе «конъюнкция-отрицание». Алгоритмы преобразования ФАЛ в ФППЗ отражены в [1].

В качестве примера представим рассматриваемую ФОСС в виде СДНФ:

$$f(x_1, \ldots, x_5) = \overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4\overline{x}_5 \vee \overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4x_5 \vee \overline{x}_1\overline{x}_2\overline{x}_3x_4\overline{x}_5 \vee \overline{x}_1\overline{x}_2\overline{x}_3x_4x_5 \vee$$
$$\vee\overline{x}_1\overline{x}_2x_3\overline{x}_4\overline{x}_5 \vee \overline{x}_1\overline{x}_2x_3\overline{x}_4x_5 \vee \overline{x}_1\overline{x}_2x_3x_4\overline{x}_5 \vee \overline{x}_1\overline{x}_2x_3x_4x_5 \vee$$
$$\vee\overline{x}_1x_2\overline{x}_3\overline{x}_4\overline{x}_5 \vee \overline{x}_1x_2\overline{x}_3\overline{x}_4x_5 \vee \overline{x}_1x_2\overline{x}_3x_4\overline{x}_5 \vee \overline{x}_1x_2\overline{x}_3x_4x_5 \vee \overline{x}_1x_2x_3\overline{x}_4\overline{x}_5 \vee$$
$$\vee\overline{x}_1x_2x_3\overline{x}_4x_5 \vee \overline{x}_1x_2x_3x_4\overline{x}_5 \vee \overline{x}_1x_2x_3x_4x_5 \vee x_1\overline{x}_2\overline{x}_3\overline{x}_4\overline{x}_5 \vee x_1\overline{x}_2\overline{x}_3\overline{x}_4x_5 \vee$$
$$\vee x_1\overline{x}_2\overline{x}_3x_4\overline{x}_5 \vee x_1\overline{x}_2\overline{x}_3x_4x_5 \vee x_1\overline{x}_2x_3\overline{x}_4\overline{x}_5 \vee x_1\overline{x}_2x_3\overline{x}_4x_5 \vee x_1\overline{x}_2x_3x_4\overline{x}_5 \vee$$
$$\vee x_1\overline{x}_2x_3x_4x_5 \vee x_1x_2\overline{x}_3\overline{x}_4\overline{x}_5 \vee x_1x_2\overline{x}_3\overline{x}_4x_5 \vee x_1x_2\overline{x}_3x_4\overline{x}_5 \vee x_1x_2\overline{x}_3x_4x_5 \vee$$
$$\vee x_1x_2x_3\overline{x}_4\overline{x}_5 \vee x_1x_2x_3\overline{x}_4x_5 \vee x_1x_2x_3x_4\overline{x}_5 \vee x_1x_2x_3x_4x_5. \quad (8)$$

Осуществим переход от логической ФОСС (8) к ее вероятностной интерпретации. При этом каждая буква в ФППЗ заменяется вероятностью ее равенства единице [12]:

$$P\{x_i = 1\} = R_i,\ P\{x_i = 0\} =$$
$$= P\{\overline{x}_i = 1\} = Q_i = 1 - R_i \quad (9)$$

– отрицание функции заменяется разностью между единицей и вероятностью равенства этой функции единице;
– операции логического умножения и сложения заменяются операциями арифметического умножения и сложения.

Тогда вероятностная функция перехода АИС ЭД в опасный режим работы будет иметь следующий вид:

$$P_{\text{прототипа}}^{f(x_1,\ldots,x_5)=1} = Q_1Q_2Q_3R_4R_5 + Q_1Q_2R_3Q_4Q_5 + Q_1Q_2R_3Q_4R_5 + \\ + Q_1Q_2R_3R_4Q_5 + Q_1Q_2R_3R_4R_5 + Q_1R_2Q_3Q_4Q_5 + Q_1R_2Q_3Q_4R_5 + \\ + Q_1R_2Q_3R_4Q_5 + Q_1R_2Q_3R_4R_5 + Q_1R_2R_3Q_4Q_5 + Q_1R_2R_3Q_4R_5 + \\ + Q_1R_2R_3R_4Q_5 + Q_1R_2R_3R_4R_5 + R_1Q_2Q_3Q_4Q_5 + R_1Q_2Q_3Q_4R_5 + \\ + R_1Q_2Q_3R_4Q_5 + R_1Q_2Q_3R_4R_5 + R_1Q_2R_3Q_4Q_5 + R_1Q_2R_3Q_4R_5 + \\ + R_1Q_2R_3R_4Q_5 + R_1Q_2R_3R_4R_5 + R_1R_2Q_3Q_4Q_5 + R_1R_2Q_3Q_4R_5 + \\ + R_1R_2Q_3R_4Q_5 + R_1R_2Q_3R_4R_5 + R_1R_2R_3Q_4Q_5 + R_1R_2R_3Q_4R_5 + \\ + R_1R_2R_3R_4Q_5 + R_1R_2R_3R_4R_5, \quad (10)$$

где: R_i – вероятность наступления события x_i ($R_i = P(x_i)$; $Q_i = 1 - R_i$).

Приняв допущение о том, что все события равновероятны, получим следующий полином, определяющий вероятность перехода АИС ЭД в опасный режим работы (нарушение целостности метаданных ЭлД):

$$P_{\text{прототипа}}^{f(x_1,\ldots,x_5)=1} = \\ = 3R^4 - R^5 - 2R^3 - 2R^2 + 3R. \quad (11)$$

При этом сумма коэффициентов полинома равна единице, что подтверждает его корректность [7].

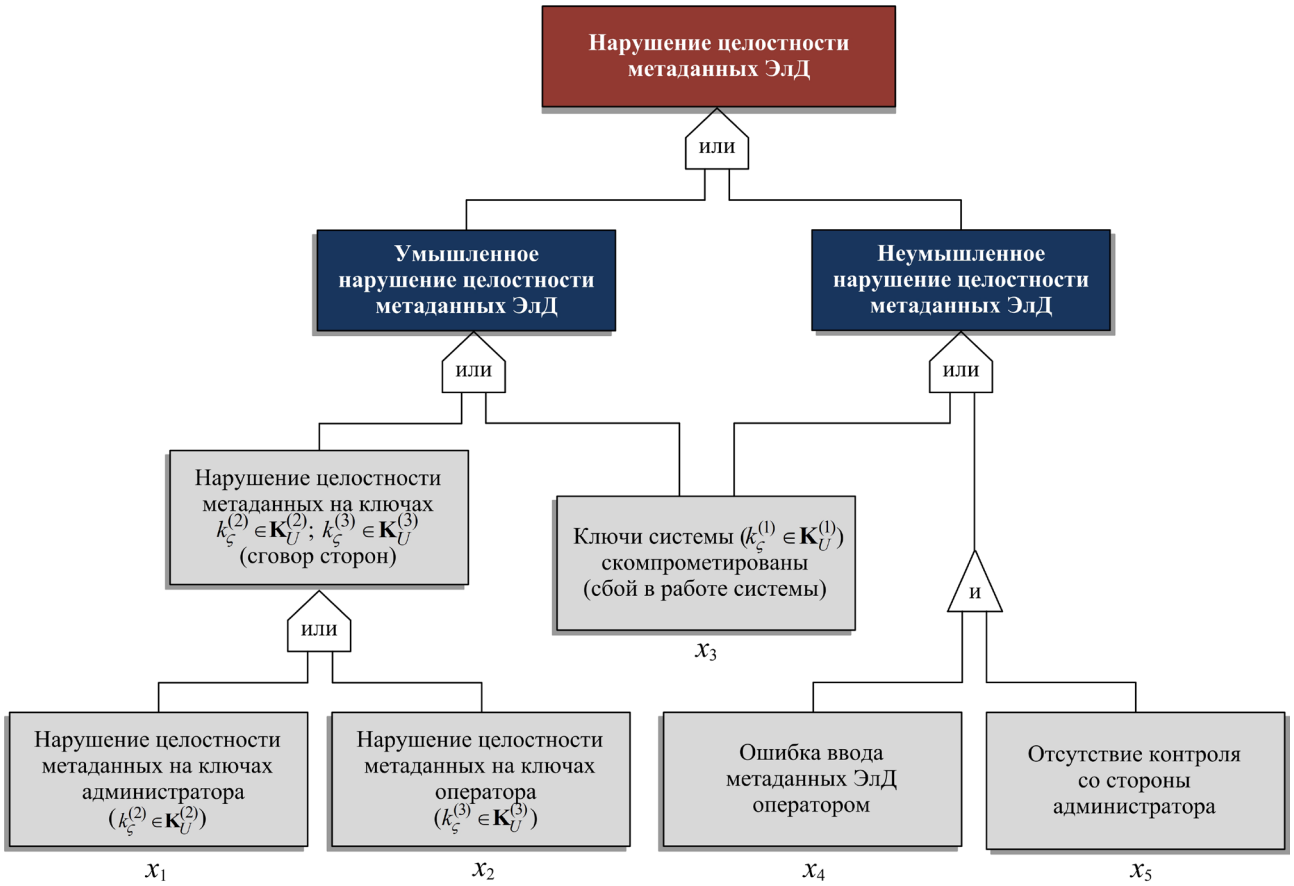

Рис. 2. Сценарий реализации угрозы нарушения целостности метаданных ЭлД при использовании хеш-функции

Рассмотрим первый вариант декомпозиции сценария перехода АИС ЭД в опасный режим работы при использовании хэш-функции (рис. 2), приводящий к умышленному нарушению целостности метаданных ЭлД уполномоченными пользователями (рис. 3).

Данному сценарию будет соответствовать следующая ФОСС:

$$f(x_1,\ x_2\ , x_3) = x_1 \vee x_2 \vee x_3. \qquad (12)$$

Представим ФОСС (12) в виде СДНФ:

$$f(x_1,\ x_2\ , x_3) = \overline{x}_1\overline{x}_2 x_3 \vee \overline{x}_1 x_2 \overline{x}_3 \vee x_1\overline{x}_2\overline{x}_3 \vee \vee x_1 x_2 x_3 \vee x_1 x_2 x_3 \vee x_1 x_2 x_3 \vee x_1 x_2 x_3. \qquad (13)$$

Запишем вероятностную функцию перехода АИС ЭД в опасный режим работы в следующем виде:

$$P_{\text{прототипа}}^{f(x_1, x_2, x_3)=1} = Q_1Q_2R_3 + Q_1R_2Q_3 + + Q_1R_2R_3 + R_1Q_2Q_3 + R_1Q_2R_3 + + R_1R_2Q_3 + R_1R_2R_3. \qquad (14)$$

При условии, что все события равновероятны, получим следующий полином, определяющий вероятность перехода АИС ЭД в опасный режим работы:

$$P_{\text{прототипа}}^{f(x_1, x_2, x_3)=1} = R^3 - 3R^2 + 3R \qquad (15)$$

Рассмотрим второй вариант декомпозиции сценария перехода АИС ЭД в опасный режим работы при использовании хеш-функции (рис. 2), приводящий к неумышленному нарушению целостности метаданных ЭлД уполномоченными пользователями (рис. 4).

Данному сценарию будет соответствовать следующая ФОСС:

$$f(x_1,\ x_2\ , x_3) = x_1 \vee\ x_2x_3. \qquad (16)$$

Представим ФОСС (16) в виде СДНФ:

$$f(x_1,\ x_2\ , x_3) = x_1\overline{x}_2\overline{x}_3 \vee \overline{x}_1 x_2 x_3 \vee x_1x_2x_3. \qquad (17)$$

Запишем вероятностную функцию перехода АИС ЭД в опасный режим работы в следующем виде:

$$P_{\text{прототипа}}^{f(x_1, x_2, x_3)=1} = R_1Q_2Q_3 + Q_1R_2R_3 + R_1R_2R_3. \qquad (18)$$

При допущении, что все события равновероятны, получим следующий полином, определяющий вероятность перехода АИС ЭД в опасный режим работы:

$$P_{\text{прототипа}}^{f(x_1, \ldots, x_3)=1} = R^2 - R^3 + R \qquad (19)$$

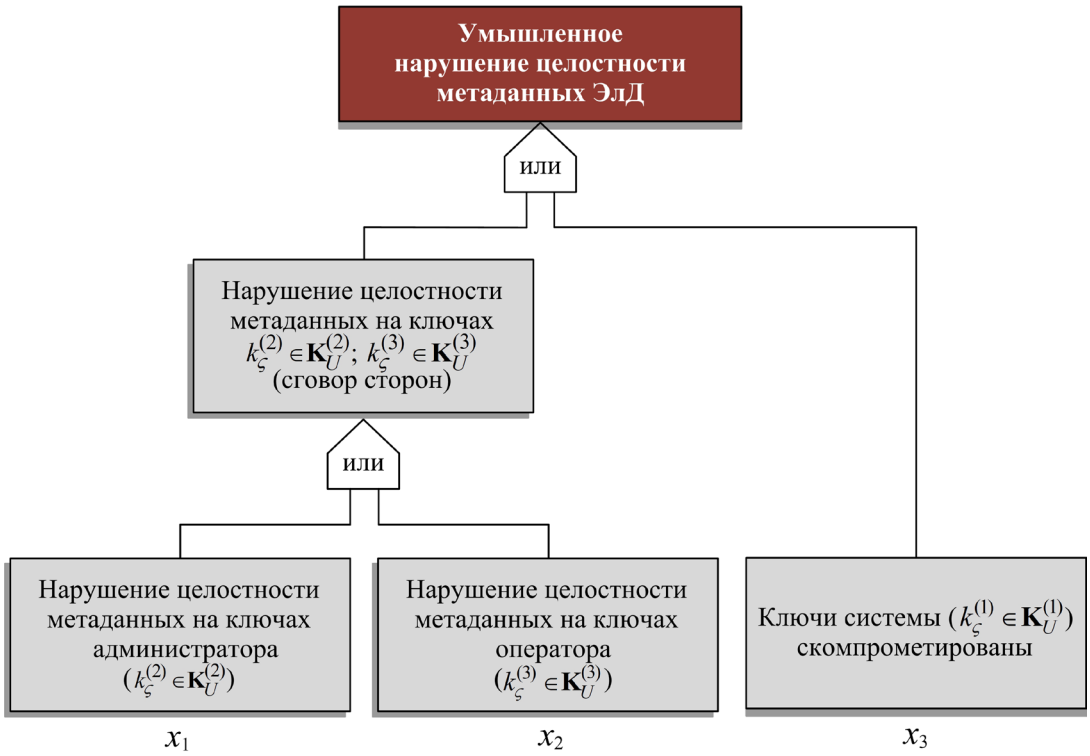

Рис. 3. Первый вариант декомпозиции сценария (рис. 2)

DOI: 10.21681/2311-3456-2021-2-37-50

Рассмотрим расширенную структуру подсистемы ЗИ АИС ЭД за счет предлагаемого криптографического рекурсивного 2-D контроля целостности метаданных ЭлД.

Вариант сценария перехода АИС ЭД с новой структурой в опасный режим работы при умышленных деструктивных воздействиях уполномоченных пользователей представлен на рис. 5.

Составим соответствующую представленному сценарию ФОСС:

$$f(x_1, \ldots, x_4) = x_1x_2x_3 \vee x_4. \quad (20)$$

Представим ФОСС (20) в виде СДНФ:

$$\begin{aligned} f(x_1, \ldots, x_4) = {} & \bar{x}_1\bar{x}_2\bar{x}_3x_4 \vee \bar{x}_1\bar{x}_2x_3x_4 \vee \\ \vee\, & \bar{x}_1x_2\bar{x}_3x_4 \vee x_1\bar{x}_2x_3\bar{x}_4 \vee x_1\bar{x}_2x_3x_4 \vee \\ \vee\, & x_1\bar{x}_2\bar{x}_3x_4 \vee x_1x_2\bar{x}_3\bar{x}_4 \vee \\ \vee\, & x_1x_2\bar{x}_3x_4 \vee x_1x_2x_3\bar{x}_4 \vee x_1x_2x_3x_4. \end{aligned} \quad (21)$$

Запишем вероятностную функцию перехода АИС ЭД в опасный режим работы в следующем виде:

$$\begin{aligned} P_{\text{раз. способа}}^{f(x_1, \ldots, x_4)=1} = {} & Q_1Q_2Q_3R_4 + Q_1Q_2R_3R_4 + \\ & + Q_1Q_2R_3R_4 + Q_1R_2Q_3R_4 + Q_1R_2R_3Q_4 + \\ & + Q_1R_2R_3R_4 + Q_1R_2R_3R_4 + R_1Q_2Q_3R_4 + \\ & + R_1Q_2R_3R_4 + R_1R_2Q_3Q_4 + R_1R_2Q_3R_4 + \\ & + R_1R_2R_3Q_4 + R_1R_2R_3R_4. \end{aligned} \quad (22)$$

При условии, что все события равновероятны, получим следующий полином, определяющий вероятность перехода АИС ЭД в опасный режим работы:

$$P_{\text{прототипа}}^{f(x_1, \ldots, x_4)=1} = R^4 - 3R^3 + 2R^2 + R. \quad (23)$$

Произведем сравнительный анализ зависимостей вероятностей перехода АИС ЭД в опасный режим работы в результате реализации угрозы умышленного нарушения целостности метаданных ЭлД от выбора структуры подсистемы ЗИ АИС ЭД (рис. 6).

Рассчитаем выигрыш разработанного способа по сравнению с использованием традиционной хеш-функции:

$$Ср.\ выигрыш = \left(1 - \frac{\int_0^{0,1} P_{\text{разр. способа}}^{f(x_i)}\, dR}{\int_0^{0,1} P_{\text{прототипа}}^{f(x_i)}\, dR}\right) \times 100\%, \quad (24)$$

где $P_{\text{прототипа}}^{f(x_i)}$ – вероятность перехода АИС ЭД в опасный режим работы при использовании хеш-функции, $P_{\text{разр. способа}}^{f(x_i)}$ – вероятность перехода АИС ЭД в опасный режим работы при использовании разработанного способа, R – вероятность события x_i.

Причем расчет выигрыша производится на практически значимом интервале вероятности перехода АИС ЭД в опасное состояние $(0;\ \ldots;\ 0,1)$, так как при переходе за его пределы инициирующее событие x_i (умышленное, неумышленное нарушение целостности метаданных ЭлД, а также их совместная реализация) будет считаться реализованным, а АИС ЭД перейдет в опасный режим работы.

Подсистема ЗИ с новой структурой, обеспечивает более высокий уровень защищенности метаданных ЭлД от умышленного нарушения целостности уполномоченными пользователями АИС ЭД (средний выигрыш составил ≈62% при $R = 0,035$).

Рассмотрим сценарий перехода АИС ЭД с новой структурой в опасный режим работы при неумышлен-

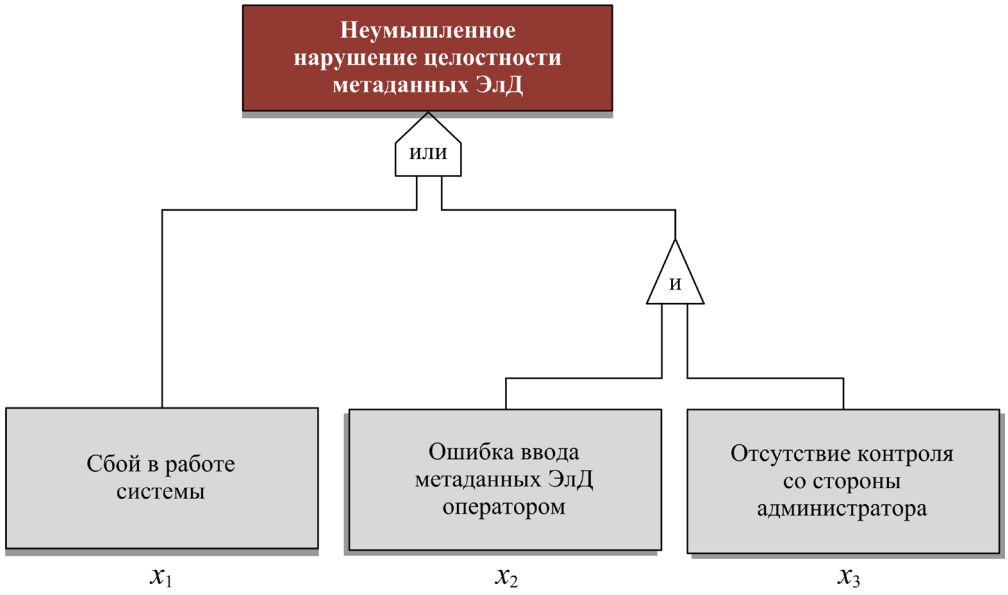

Рис. 4. Второй вариант декомпозиции сценария (рис. 2)

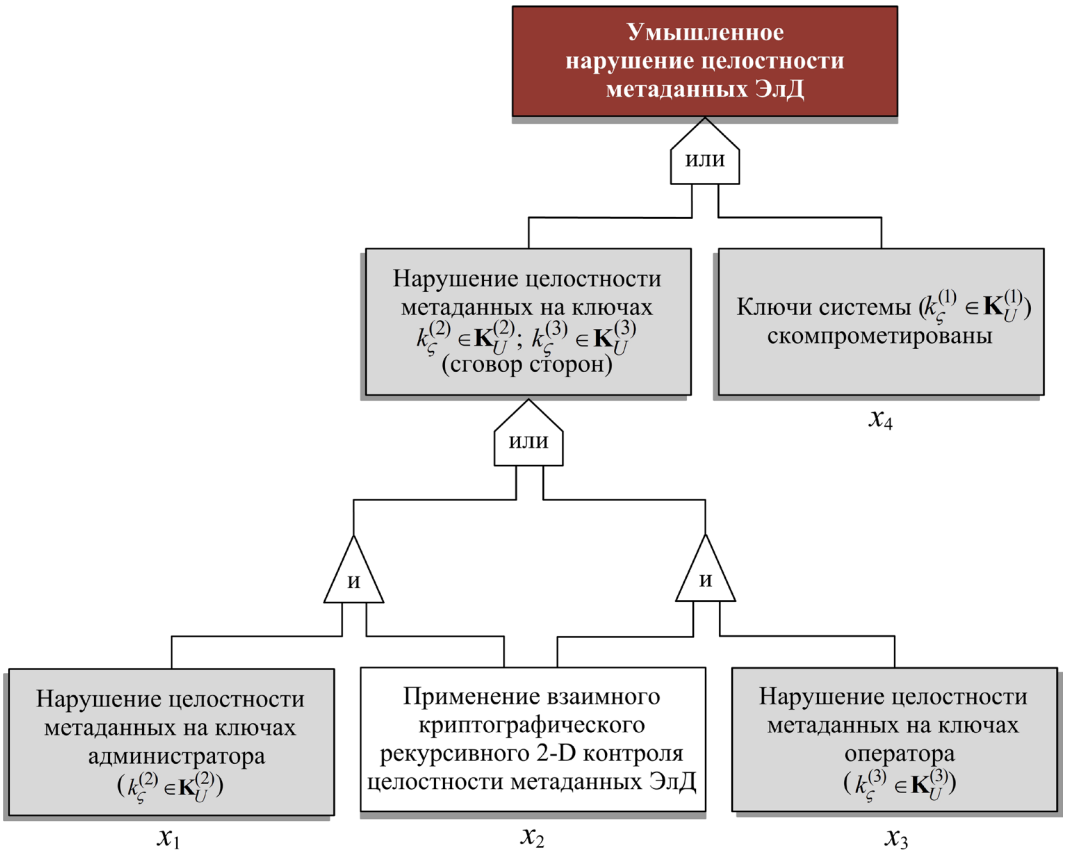

Рис. 5. Сценарий реализации угрозы умышленного нарушения целостности метаданных ЭлД при использовании разработанного решения

ных деструктивных воздействиях уполномоченных пользователей (рис. 7).

Данному сценарию соответствует следующая ФОСС:

$$f(x_1, \ldots, x_4) = x_1 \vee x_2 x_3 x_4. \qquad (25)$$

Представим ФОСС (25) в виде СДНФ:

$$f(x_1, \ldots, x_4) = \bar{x}_1 x_2 \bar{x}_3 \bar{x}_4 \vee \bar{x}_1 x_2 x_3 x_4 \vee x_1 \bar{x}_2 x_3 \bar{x}_4 \vee \vee \bar{x}_1 x_2 x_3 x_4 \vee x_1 \bar{x}_2 x_3 x_4 \vee \vee x_1 x_2 \bar{x}_3 \bar{x}_4 \vee x_1 x_2 \bar{x}_3 x_4 \vee \vee x_1 x_2 x_3 \bar{x}_4 \vee x_1 x_2 x_3 x_4. \qquad (26)$$

Вероятностная функция перехода АИС ЭД в опасный режим работы примет вид:

$$P_{\text{разр. способа}}^{f(x_1, \ldots, x_4)=1} = Q_1 R_2 Q_3 Q_4 + Q_1 R_2 Q_3 R_4 + + Q_1 R_2 Q_3 R_4 + Q_1 R_2 R_3 Q_4 + Q_1 R_2 R_3 R_4 + + R_1 Q_2 R_3 R_4 + R_1 R_2 Q_3 Q_4 + R_1 R_2 Q_3 R_4 + + R_1 R_2 R_3 Q_4 + R_1 R_2 R_3 R_4. \qquad (27)$$

При условии, что все события равновероятны, получим следующий полином, определяющий вероятность перехода АИС ЭД в опасный режим работы:

$$P_{\text{разр. способа}}^{f(x_1, \ldots, x_4)=1} = 3R^2 - 2R^3 + R(1-R)^3. \qquad (28)$$

Произведем сравнительный анализ зависимостей вероятностей перехода АИС ЭД в опасный режим работы, в результате реализации угрозы неумышленного нарушения целостности метаданных ЭлД, от выбора структуры подсистемы ЗИ АИС ЭД (рис. 8).

Подсистема ЗИ с новой структурой, обеспечивает более высокий уровень защищенности метаданных ЭлД от неумышленного нарушения целостности уполномоченными пользователями АИС ЭД (средний выигрыш составил ≈3% при $R = 0{,}009$).

В целях получения итоговой оценки результатов исследования произведем сравнительный анализ зависимостей вероятностей перехода АИС ЭД в опасный режим работы, в результате реализации угрозы совместного осуществления умышленного и неумышленного нарушения целостности метаданных ЭлД уполномоченными пользователями с учетом расширенной структуры подсистемы ЗИ АИС ЭД. Для чего построим соответствующий сценарий перехода АИС ЭД в опасный режим работы (рис. 9).

Составим, соответствующую итоговому сценарию, ФОСС:

$$f(x_1, \ldots, x_6) = x_1 x_2 x_3 \vee x_4 \vee x_2 x_5 x_6. \qquad (29)$$

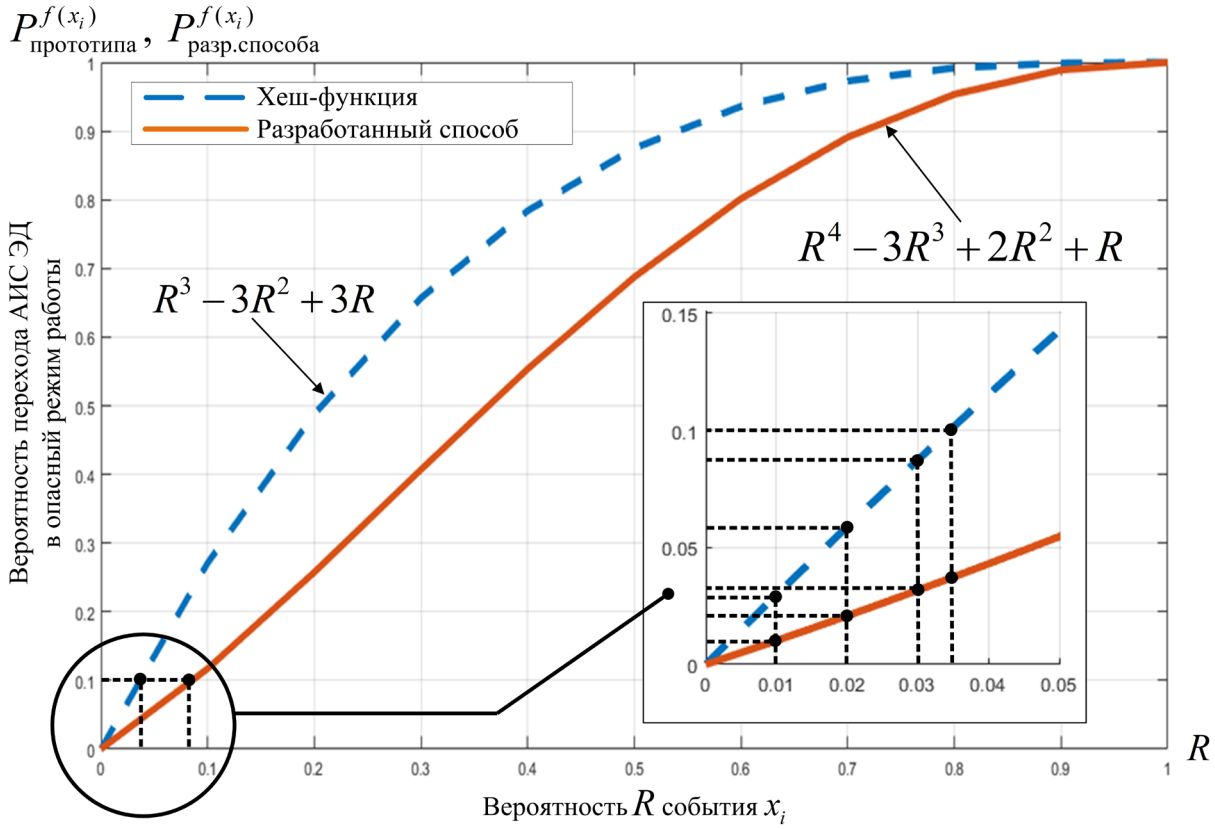

Рис. 6. Сравнительный анализ зависимостей вероятностей перехода АИС ЭД в опасный режим работы в результате реализации угрозы умышленного нарушения целостности метаданных ЭлД от выбора структуры подсистемы ЗИ АИС ЭД

Рис. 7. Сценарий реализации угрозы неумышленного нарушения целостности метаданных ЭлД при использовании разработанного решения

Представим ФОСС (29) в виде СДНФ:

$$
\begin{aligned}
f(x_1,\ \ldots,x_6) = {} & \bar{x}_1\bar{x}_2\bar{x}_3x_4\bar{x}_5\bar{x}_6 \vee \bar{x}_1\bar{x}_2\bar{x}_3x_4\bar{x}_5x_6 \vee \bar{x}_1\bar{x}_2\bar{x}_3x_4x_5\bar{x}_6 \vee \bar{x}_1\bar{x}_2\bar{x}_3x_4x_5x_6 \vee \\
& \vee \bar{x}_1\bar{x}_2x_3x_4\bar{x}_5\bar{x}_6 \vee \bar{x}_1\bar{x}_2x_3x_4\bar{x}_5x_6 \vee \bar{x}_1\bar{x}_2x_3x_4x_5\bar{x}_6 \vee \bar{x}_1\bar{x}_2x_3x_4x_5x_6 \vee \bar{x}_1x_2\bar{x}_3\bar{x}_4x_5x_6 \vee \\
& \vee \bar{x}_1x_2\bar{x}_3x_4\bar{x}_5\bar{x}_6 \vee \bar{x}_1x_2\bar{x}_3x_4\bar{x}_5x_6 \vee \bar{x}_1x_2\bar{x}_3x_4x_5\bar{x}_6 \vee \bar{x}_1x_2\bar{x}_3x_4x_5x_6 \vee \bar{x}_1x_2x_3\bar{x}_4\bar{x}_5\bar{x}_6 \vee \\
& \vee \bar{x}_1x_2x_3\bar{x}_4\bar{x}_5x_6 \vee \bar{x}_1x_2x_3\bar{x}_4x_5\bar{x}_6 \vee \bar{x}_1x_2x_3\bar{x}_4x_5x_6 \vee \bar{x}_1x_2x_3x_4\bar{x}_5\bar{x}_6 \vee \bar{x}_1x_2x_3x_4\bar{x}_5x_6 \vee \\
& \vee \bar{x}_1x_2x_3x_4x_5\bar{x}_6 \vee \bar{x}_1x_2x_3x_4x_5x_6 \vee x_1\bar{x}_2\bar{x}_3x_4\bar{x}_5\bar{x}_6 \vee x_1\bar{x}_2\bar{x}_3x_4\bar{x}_5x_6 \vee x_1\bar{x}_2\bar{x}_3x_4x_5\bar{x}_6 \vee \\
& \vee x_1\bar{x}_2\bar{x}_3x_4x_5x_6 \vee x_1\bar{x}_2x_3x_4\bar{x}_5\bar{x}_6 \vee x_1\bar{x}_2x_3x_4\bar{x}_5x_6 \vee x_1\bar{x}_2x_3x_4x_5\bar{x}_6 \vee x_1\bar{x}_2x_3x_4x_5x_6 \vee \\
& \vee x_1x_2\bar{x}_3\bar{x}_4\bar{x}_5\bar{x}_6 \vee x_1x_2\bar{x}_3\bar{x}_4\bar{x}_5x_6 \vee x_1x_2\bar{x}_3\bar{x}_4x_5\bar{x}_6 \vee x_1x_2\bar{x}_3\bar{x}_4x_5x_6 \vee x_1x_2\bar{x}_3x_4\bar{x}_5\bar{x}_6 \vee \\
& \vee x_1x_2\bar{x}_3x_4\bar{x}_5x_6 \vee x_1x_2\bar{x}_3x_4x_5\bar{x}_6 \vee x_1x_2\bar{x}_3x_4x_5x_6 \vee x_1x_2x_3\bar{x}_4\bar{x}_5\bar{x}_6 \vee x_1x_2x_3\bar{x}_4\bar{x}_5x_6 \vee \\
& \vee x_1x_2x_3\bar{x}_4x_5\bar{x}_6 \vee x_1x_2x_3\bar{x}_4x_5x_6 \vee x_1x_2x_3x_4\bar{x}_5\bar{x}_6 \vee x_1x_2x_3x_4\bar{x}_5x_6 \vee x_1x_2x_3x_4x_5\bar{x}_6 \vee \\
& \vee x_1x_2x_3x_4x_5x_6.
\end{aligned} \tag{30}
$$

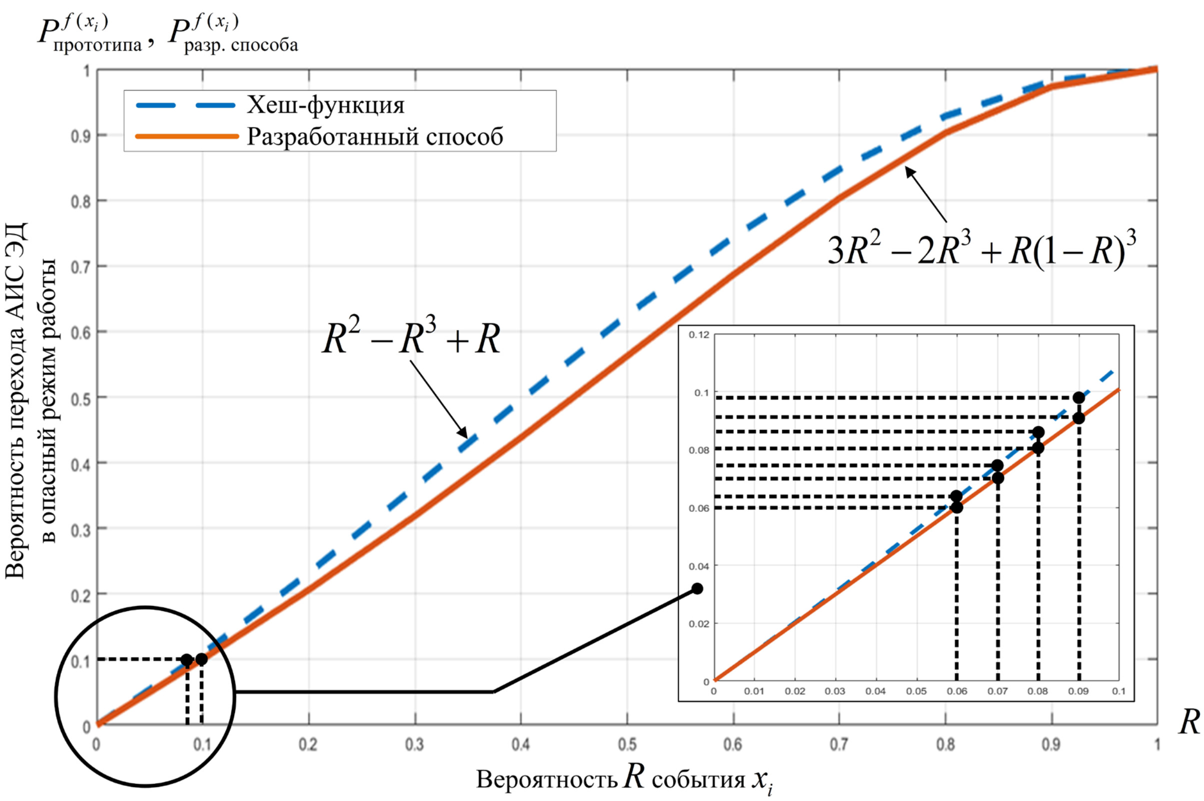

Рис. 8. Сравнительный анализ зависимостей вероятностей перехода АИС ЭД в опасный режим работы в результате реализации угрозы неумышленного нарушения целостности метаданных ЭлД от выбора структуры подсистемы ЗИ АИС ЭД

DOI: 10.21681/2311-3456-2021-2-37-50

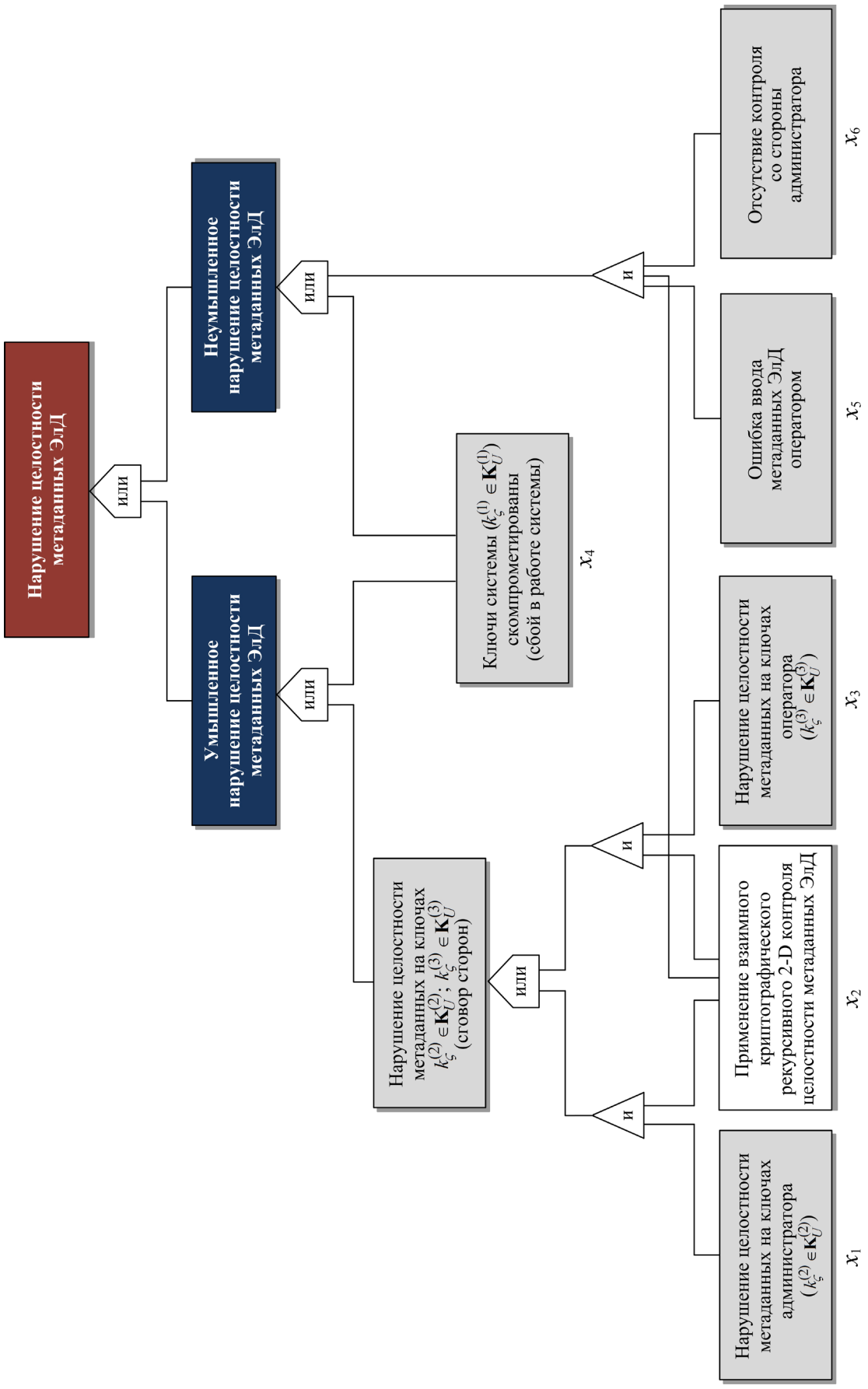

Рис. 9. Сценарий реализации угрозы при совместном осуществлении умышленного и неумышленного нарушения целостности метаданных ЭлД при использовании разработанного решения

Запишем вероятностную функцию перехода АИС ЭД в опасный режим работы:

$$
\begin{aligned}
P_{\text{разр. способа}}^{f(x_1,\ldots,x_6)=1} &= Q_1Q_2Q_3R_4Q_5Q_6 + Q_1Q_2Q_3R_4Q_5R_6 + Q_1Q_2Q_3R_4R_5Q_6 + \\
&+Q_1Q_2Q_3R_4R_5R_6 + Q_1Q_2R_3R_4Q_5Q_6 + Q_1Q_2R_3R_4Q_5R_6 + Q_1Q_2R_3R_4R_5Q_6 + \\
&+Q_1Q_2R_3R_4R_5R_6 + Q_1R_2Q_3Q_4R_5R_6 + Q_1R_2Q_3R_4Q_5Q_6 + Q_1R_2Q_3R_4Q_5R_6 + \\
&+Q_1R_2Q_3R_4R_5Q_6 + Q_1R_2Q_3R_4R_5R_6 + Q_1R_2R_3Q_4Q_5Q_6 + Q_1R_2R_3Q_4Q_5R_6 + \\
&+Q_1R_2R_3Q_4R_5Q_6 + Q_1R_2R_3Q_4R_5R_6 + Q_1R_2R_3R_4Q_5Q_6 + Q_1R_2R_3R_4Q_5R_6 + \\
&+Q_1R_2R_3R_4R_5Q_6 + Q_1R_2R_3R_4R_5R_6 + R_1Q_2Q_3R_4Q_5Q_6 + R_1Q_2Q_3R_4Q_5R_6 + \\
&+R_1Q_2Q_3R_4R_5Q_6 + R_1Q_2Q_3R_4R_5R_6 + R_1Q_2R_3R_4Q_5Q_6 + R_1Q_2R_3R_4Q_5R_6 + \\
&+R_1Q_2R_3R_4R_5Q_6 + R_1Q_2R_3R_4R_5R_6 + R_1R_2Q_3Q_4Q_5Q_6 + R_1R_2Q_3Q_4Q_5R_6 + \\
&+R_1R_2Q_3Q_4R_5Q_6 + R_1R_2Q_3Q_4R_5R_6 + R_1R_2Q_3R_4Q_5Q_6 + R_1R_2Q_3R_4Q_5R_6 + \\
&+R_1R_2Q_3R_4R_5Q_6 + R_1R_2Q_3R_4R_5R_6 + R_1R_2R_3Q_4Q_5Q_6 + R_1R_2R_3Q_4Q_5R_6 + \\
&+R_1R_2R_3Q_4R_5Q_6 + R_1R_2R_3Q_4R_5R_6 + R_1R_2R_3R_4Q_5Q_6 + R_1R_2R_3R_4Q_5R_6 + \\
&+R_1R_2R_3R_4R_5Q_6 + R_1R_2R_3R_4R_5R_6.
\end{aligned}
\tag{31}
$$

При условии, что все события равновероятны, получим следующий полином, определяющий вероятность перехода АИС ЭД в опасный режим работы:

$$
\begin{aligned}
P_{\text{разр. способа}}^{f(x_1,\ldots,x_6)=1} &= 3R^5 - R^6 - \\
&- 2R^4 - 2R^3 + 2R^2 + R \quad .
\end{aligned}
\tag{32}
$$

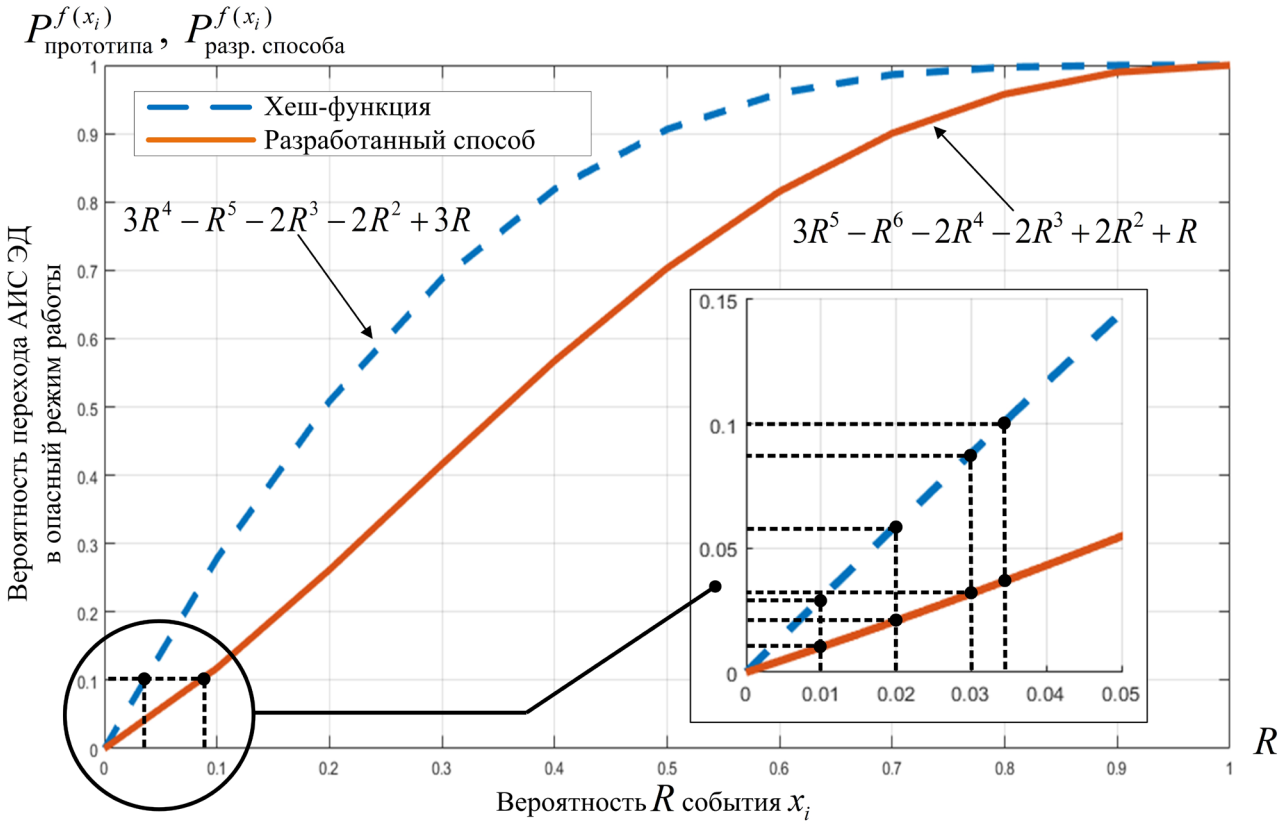

Рис. 10. Сравнительный анализ зависимостей вероятностей перехода АИС ЭД в опасный режим работы в результате реализации угрозы совместного осуществления умышленного и неумышленного нарушения целостности метаданных ЭлД от выбора структуры подсистемы ЗИ АИС ЭД

DOI: 10.21681/2311-3456-2021-2-37-50

Построим графики зависимостей вероятностей перехода АИС ЭД в опасный режим работы в результате реализации угрозы совместного осуществления умышленного и неумышленного нарушения целостности метаданных ЭлД уполномоченными пользователями с учетом расширенной структуры подсистемы ЗИ АИС ЭД (рис. 10).

Результаты сравнительного анализа показывают, что подсистема ЗИ с новой структурой обеспечивает более высокий уровень защищенности метаданных ЭлД от совместного осуществления умышленного и неумышленного нарушения целостности уполномоченными пользователями АИС ЭД (средний выигрыш составил ≈67% при $R = 0,034$). Выигрыш получен за счет усложнения процедуры контроля целостности метаданных ЭлД, обрабатываемых АИС ЭД. При этом полиномиальная сложность предложенного решения не снижает основных показателей эффективности АИС ЭД (работоспособность, производительность, оперативность и т.д.).

Таким образом, исходными данными для логико-вероятностных моделей АИС ЭД являются вероятности истинности отдельных аргументов в ФАЛ, описывающих работоспособное состояние системы или ее переход в опасный режим работы (нарушение целостности метаданных ЭлД) [13].

Выводы

Итогом проведенного исследования стала оценка уровня защищенности метаданных ЭлД, обрабатываемых АИС ЭД, показателем которого выбрана вероятность нарушения их целостности. Сравнительный анализ разработанного способа с традиционно используемой хэш-функцией, проведенный на основе ЛВМ, показал общий выигрыш в 67% при заданных допущениях, что свидетельствует об успешном достижении поставленных целей [16-18].

Литература

1. Рябинин И.А., Соложенцева Е.Д., Карасева В.В. Путеводитель по логико-вероятностному исчислению // Моделирование и анализ безопасности и риска в сложных системах. Труды Международной научной школы МАБР-2016, 2016. С. 9-25.
2. Демин А.В. Логико-вероятностный метод управления модульными роботами // Системная информатика. 2017. № 11. С. 61-80.
3. Селуянов М.Н. Применение общего логико-вероятностного метода при моделировании функционирования ответственных систем // Вестник Концерна ВКО Алмаз-Антей. 2017. № 2 (21). С. 49-55.
4. Коцыняк М.А., Лаута О.С., Иванов Д.А., Лукина О.М. Методика оценки эффективности защиты информационно-телекоммуникационной сети в условиях таргетированных кибернетических атак // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2018. № 11-12 (125-126). С. 71-79.
5. Скобцов В.Ю., Кругликов С.В., Ким Д.С. и др. Анализ показателей надежности, живучести и телеметрии бортовой аппаратуры малых космических аппаратов // Вопросы кибербезопасности. 2018. № 4 (28). С. 54-69. DOI: 10.21681/2311-3456-2018-4-54-69.
6. Glazunov V.V., Kurochkin M.A., Popov S.G. Qualification routes messaging for dynamic systems using a logical-probabilistic method // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2015. № 1 (212). С. 16-21.
7. Рябинин И.А. Логико-вероятностный метод и его практическое использование // Моделирование и анализ безопасности и риска в сложных системах. Труды Международной научной школы МАБР-2015, 2015. С. 19-26.
8. Елисеев Н.И., Тали Д.И., Обланенко А.А. Оценка уровня защищенности автоматизированных информационных систем юридически значимого электронного документооборота на основе логико-вероятностного метода // Вопросы кибербезопасности. 2019. № 6 (34). С. 7-14. DOI: 10.21681/2311-3456-2019-6-07-16.
9. Тали Д.И. Модель угроз безопасности метаданным в системе электронного документооборота военного назначения // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2020. № 139-140. С. 95-101.
10. Елисеев Н.И., Финько О.А. Теоретические аспекты развития системы электронного документооборота Министерства обороны Российской Федерации // Военно-теоретический журнал «Военная мысль», 2015. № 7. С. 55-63.
11. Елисеев Н.И. Модель угроз безопасности информации при ее обработке в системе защищенного электронного документооборота // Известия ЮФУ. Технические науки. Тематический выпуск «Информационная безопасность», № 12 (137). Таганрог: ТТИ ЮФУ, 2012. С. 212-218.
12. Рябинин И.А., Струков А.В. Решение одной задачи оценки надежности структурно-сложной системы разными логико-вероятностными методами // Моделирование и анализ безопасности и риска в сложных системах. Труды Международной научной школы МАБР-2019 , 2019. С. 159-172.
13. Финько О.А., Соколовский Е.П. Алгоритм оценки риска информационной безопасности в системах защиты информации на основе логико-вероятностного метода И.А. Рябинина // Известия ЮФУ. Технические науки. Тематический выпуск «Информационная безопасность», № 12 (149). Таганрог: ТТИ ЮФУ, 2013. С. 172-180.
14. Макаренко А.В., Шипилов А.П. Логико-вероятностные методы в расчетах показателей надежности // Воронежский научно-технический Вестник. 2015. Т. 4. № 3-3 (13). С. 122-126.
15. Рябинин И.А. Надежность и безопасность структурно-сложных систем / Политехника. Издательство Санкт-Петербургского университета. СПб, 2012. 276 с.
16. Тали Д.И., Финько О.А. Криптографический рекурсивный контроль целостности метаданных электронных документов. Часть 1. Математическая модель // Вопросы кибербезопасности. 2020. № 5 (39). С. 2-18. DOI: 10.21681/2311-3456-2020-05-2-18.

17. Тали Д.И., Финько О.А. Криптографический рекурсивный контроль целостности метаданных электронных документов. Часть 2. Комплекс алгоритмов // Вопросы кибербезопасности. 2020. № 6 (40). С. 32-47. DOI: 10.21681/2311-3456-2020-06-32-47.
18. Тали Д.И., Финько О.А. Криптографический рекурсивный контроль целостности метаданных электронных документов. Часть 3. Методика применения // Вопросы кибербезопасности. 2021. № 1 (41). С. 18-29. DOI: 10.21681/2311-3456-2021-1-18-29

CRYPTOGRAPHIC RECURSIVE CONTROL OF INTEGRITY OF METADATA ELECTRONIC DOCUMENTS. PART 4. EVALUATION OF RESULTS

Tali D.I. [3]***, Finko O.A.*** [4]

The purpose *of the study is to obtain a numerical assessment of the results of the application, previously presented by the authors, of the method of cryptographic recursive 2-D control of the integrity of the metadata of electronic documents.*

Research methods: *logical-probabilistic method I.A. Ryabinin.*

Research result: *a necessary condition for maintaining the integrity of electronic documents processed by automated information systems for electronic document management is to ensure the required level of metadata security. To evaluate the research results, the probability of violation of the integrity of electronic documents (through destructive influences of authorized users on metadata) was chosen as an indicator of efficiency.*

The presented approach to the construction of logical-probabilistic models for assessing the level of security of metadata of electronic documents allows in practice to obtain numerical values of the probabilities of transition of the systems under consideration to a dangerous state (associated with a violation of the integrity of the metadata of electronic documents), taking into account the structure of such systems and the real conditions of their functioning.

The effect of using the developed method, under the conditions of destructive influences of authorized users (insiders), in comparison with the known solutions (using a hash function) of such problems, is 67% under the given assumptions.

Keywords: *structurally complex systems, automated information systems, electronic document management, security of metadata, algebra of logic, theory of probability, function of a dangerous state of the system, scenario of system functioning, hash function.*

References

1. Ryabinin I.A., Solozhentseva Ye.D., Karaseva V.V. Putevoditel' po logiko-veroyatnostnomu ischisleniyu // Modelirovaniye i analiz bezopasnosti i riska v slozhnykh sistemakh. Trudy Mezhdunarodnoy nauchnoy shkoly MABR-2016, 2016. S. 9-25.
2. Demin A.V. Logiko-veroyatnostnyy metod upravleniya modul'nymi robotami // Sistemnaya informatika. 2017. № 11. S. 61-80.
3. Seluyanov M.N. Primeneniye obshchego logiko-veroyatnostnogo metoda pri modelirovanii funktsionirovaniya otvetstvennykh sistem // Vestnik Kontserna VKO Almaz-Antey. 2017. № 2 (21). S. 49-55.
4. Kotsynyak M.A., Lauta O.S., Ivanov D.A., Lukina O.M. Metodika otsenki effektivnosti zashchity informatsionno-telekommunikatsionnoy seti v usloviyakh targetirovannykh kiberneticheskikh atak // Voprosy oboronnoy tekhniki. Seriya 16: Tekhnicheskiye sredstva protivodeystviya terrorizmu. 2018. № 11-12 (125-126). S. 71-79.
5. Skobtsov V.YU., Kruglikov S.V., Kim D.S. i dr. Analiz pokazateley nadezhnosti, zhivuchesti i telemetrii bortovoy apparatury malykh kosmicheskikh apparatov // Voprosy kiberbezopasnosti. 2018. № 4 (28). S. 54-69. DOI: 10.21681/2311-3456-2018-4-54-69
6. Glazunov V.V., Kurochkin M.A., Popov S.G. Qualification routes messaging for dynamic systems using a logical-probabilistic method

3 Dmitry Tali, postgraduate student of department 21 (tactical and special communication) special, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: dimatali@mail.ru

4 Oleg Finko, Dr.Sc., Professor, Professor of department 22 (special communication technology), Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, professor of the Department of Information Security of Automated Systems, North Caucasus Federal University, Academic Advisor of the Russian Academy of Rocket and Artillery Sciences (RARAN), Krasnodar, Russia. E-mail: ofinko@yandex.ru. Web: http://www.mathnet.ru/person40004. ORCID 0000-0002-7376-2714

// Nauchno-tekhnicheskiye vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Informatika. Telekommunikatsii. Upravleniye. 2015. № 1 (212). S. 16-21.
7. Ryabinin I.A. Logiko-veroyatnostnyy metod i yego prakticheskoye ispol'zovaniye // Modelirovaniye i analiz bezopasnosti i riska v slozhnykh sistemakh. Trudy Mezhdunarodnoy nauchnoy shkoly MABR-2015, 2015. S. 19-26.
8. Yeliseyev N.I., Tali D.I., Oblanenko A.A. Otsenka urovnya zashchishchennosti avtomatizirovannykh informatsionnykh sistem yuridicheski znachimogo elektronnogo dokumentooborota na osnove logiko-veroyatnostnogo metoda // Voprosy kiberbezopasnosti. 2019. № 6 (34). S. 7-14. DOI: 10.21681/2311-3456-2019-6-07-16.
9. Tali D.I. Model' ugroz bezopasnosti metadannym v sisteme elektronnogo dokumentooborota voyennogo naznacheniya // Voprosy oboronnoy tekhniki. Seriya 16: Tekhnicheskiye sredstva protivodeystviya terrorizmu. 2020. № 139-140. S. 95-101.
10. Yeliseyev N.I., Finko O.A. Teoreticheskiye aspekty razvitiya sistemy elektronnogo dokumentooborota Ministerstva oborony Rossiyskoy Federatsii // Voyenno-teoreticheskiy zhurnal «Voyennaya mysl'», 2015. № 7. S. 55-63.
11. Yeliseyev N.I. Model' ugroz bezopasnosti informatsii pri yeye obrabotke v sisteme zashchishchennogo elektronnogo dokumentooborota // Izvestiya YUFU. Tekhnicheskiye nauki. Tematicheskiy vypusk «Informatsionnaya bezopasnost'», № 12 (137). Taganrog: TTI YUFU, 2012. S. 212-218.
12. Ryabinin I.A., Strukov A.V. Resheniye odnoy zadachi otsenki nadezhnosti strukturno-slozhnoy sistemy raznymi logiko-veroyatnostnymi metodami // Modelirovaniye i analiz bezopasnosti i riska v slozhnykh sistemakh. Trudy Mezhdunarodnoy nauchnoy shkoly MABR-2019 , 2019. S. 159-172.
13. Fin'ko O.A., Sokolovskiy Ye.P. Algoritm otsenki riska informatsionnoy bezopasnosti v sistemakh zashchity informatsii na osnove logiko-veroyatnostnogo metoda I.A. Ryabinina // Izvestiya YUFU. Tekhnicheskiye nauki. Tematicheskiy vypusk «Informatsionnaya bezopasnost'», № 12 (149). Taganrog: TTI YUFU, 2013. S. 172-180.
14. Makarenko A.V., Shipilov A.P. Logiko-veroyatnostnyye metody v raschetakh pokazateley nadezhnosti // Voronezhskiy nauchno-tekhnicheskiy Vestnik. 2015. T. 4. № 3-3 (13). S. 122-126.
15. Ryabinin I.A. Nadezhnost' i bezopasnost' strukturno-slozhnykh sistem / Politekhnika. Izdatel'stvo Sankt-Peterburgskogo universiteta. SPb, 2012. S. 276.
16. Tali D.I., Fin'ko O.A. Kriptograficheskiy rekursivnyy kontrol' tselostnosti metadannykh elektronnykh dokumentov. Chast' 1. Matematicheskaya model' // Voprosy kiberbezopasnosti. 2020. № 5 (39). S. 2-18. DOI: 10.21681/2311-3456-2020-05-2-18.
17. Tali D.I., Fin'ko O.A. Kriptograficheskiy rekursivnyy kontrol' tselostnosti metadannykh elektronnykh dokumentov. Chast' 2. Kompleks algoritmov // Voprosy kiberbezopasnosti. 2020. № 6 (40). S. 32-47. DOI: 10.21681/2311-3456-2020-06-32-47.
18. Tali D.I., Fin'ko O.A. Kriptograficheskiy rekursivnyy kontrol' tselostnosti metadannykh elektronnykh dokumentov. Chast' 3. Metodika primeneniya // Voprosy kiberbezopasnosti. 2021. № 1 (41). S. 18-29. DOI: 10.21681/2311-3456-2021-1-18-29