Development of the Theoretical Approach Based on Matrix Theory for Analyzing the State of Information Security Systems

Bobok I.I.[1], Kobozeva A.A.[2]
[1]Odesa Polytechnic National University
[2]Odesa I.I.Mechnikov National University
Odesa, Ukraine

Abstract. The widespread introduction of information technologies into all spheres of society, the creation of a significant amount of confidential and critical data in digital form leads to an increase in the priority of information security tasks everywhere, including in the energy sector, which relates to the critical infrastructure of any state. The purpose of the work is to develop the mentioned approach to ensure the possibility of increasing the efficiency of information security methods based on it. The goal was achieved through a detailed study of disturbances in the values of formal parameters that uniquely determine the matrix that is assigned to the information security system under conditions of active attacks (disturbances) on the system. Singular numbers and singular vectors of the matrix are considered as such parameters. The most important result of the work is the substantiation of the existence and establishment of interconnected regions of stabilization of disturbances of singular numbers and singular vectors of the system matrix, while the region of stabilization of singular numbers corresponds to the region of monotonous decrease in their disturbances with increasing numbers, while the stabilization of singular vectors corresponds to the region in which their disturbances are comparable with 90 degrees. It is shown that the stabilization process is determined by the mathematical properties of the parameters under consideration. The significance of the obtained result lies in the possibility of using it to improve various information security systems that were built or studied using a general approach to analyzing their state, both theoretically and practically. The work provides examples of such use.
Keywords: information protection system, singular vector, singular number, sensitivity, active attack.

DOI: https://doi.org/10.52254/1857-0070.2024.3-63.03
UDC: 004.056

Dezvoltarea unei abordări teoretice bazată pe teoria matricelor pentru analiza stării sistemelor de securitate a informației

Bobok I.I.[1], Kobozeva A.A.[2]
[1]Universitatea Națională Politehnică din Odessa, [2]Universitatea Națională de Stat din Odesa, Odesa, Ucraina

Abstract. Introducerea pe scară largă a tehnologiilor informaționale în toate sferele societății, crearea unei cantități semnificative de date confidențiale și critice în formă digitală duce la o creștere a priorității sarcinilor de securitate a informațiilor peste tot, inclusiv în sectorul energetic, care se referă la aspectele critice. Infrastructura oricărui stat. Eficacitatea securității informațiilor depinde în mod esențial de baza teoretică, care stă la baza metodelor și algoritmilor utilizați.Scopul lucrării este de a dezvolta abordarea menționată pentru a asigura posibilitatea creșterii eficienței metodelor de securitate a informațiilor bazate pe aceasta. Scop a fost atins printr-un studiu detaliat al perturbărilor în valorile parametrilor formali care determină în mod unic matricea care este alocată sistemului de securitate a informațiilor în condiții de atacuri active (perturbații) asupra sistemului. Numerele singulare și vectorii singulari ai matricei sunt considerați astfel de parametri. Cel mai important rezultat al lucrării este fundamentarea existenței și stabilirii unor regiuni interconectate de stabilizare a perturbațiilor numerelor singulare și ale vectorilor singulari ai matricei sistemului, în timp ce regiunea de stabilizare a numerelor singulare corespunde regiunii de scădere monotonă a acestora. Perturbații cu număr tot mai mare, în timp ce stabilizarea vectorilor singulari corespunde regiunii în care perturbațiile lor sunt comparabile cu 90 de grade. Se arată că procesul de stabilizare este determinat de proprietățile matematice ale parametrilor luați în considerare. Semnificația rezultatului obținut constă în posibilitatea utilizării acestuia pentru îmbunătățirea diferitelor sisteme de securitate a informațiilor care sunt construite sau studiate folosind o abordare generală a analizei stării acestora, atât teoretic cât și practic. Lucrarea oferă exemple de astfel de utilizare.
***Keywords*:** sistem de securitate a informației, vector singular, număr singular, sensibilitate, atac activ.

Развитие теоретического подхода, основанного на теории матриц, для анализа состояния систем защиты информации

Бобок И.И.[1], Кобозева А.А.[2]
[1]Национальный университет «Одесская политехника»
[2]Одесский национальный университет им. И.И.Мечникова
Одесса, Украина

Аннотация. Широкое внедрение информационных технологий во все сферы жизни общества, создание значительного объема конфиденциальных и критически важных данных в цифровом виде приводит к росту приоритета задач информационной безопасности повсеместно, в том числе в сфере энергетики, относящейся к критической инфраструктуре любого государства. Эффективность обеспечения защиты информации ключевым образом зависит от теоретического базиса, который положен в основу используемых методов и алгоритмов. Существующие теоретические подходы не удовлетворяют в полной мере современным вызовам в области информационной безопасности. Хорошо зарекомендовал себя для решения задач защиты информации общий подход к анализу состояния информационных систем, основанный на теории матриц, однако и он не устраняет все теоретические проблемы рассматриваемой области. Целью работы является развитие упомянутого подхода для обеспечения возможности повышения эффективности методов защиты информации, основывающихся на нем. Цель была достигнута путем детального исследования возмущений значений формальных параметров, однозначно определяющих матрицу, которая ставится в соответствие системе защиты информации, в условиях активных атак (возмущающих воздействий) на систему. В качестве таких параметров рассматриваются сингулярные числа и сингулярные векторы матрицы. Наиболее важным результатом работы является обоснование существования и установление взаимосвязанных областей стабилизации возмущений сингулярных чисел и сингулярных векторов матрицы системы, при этом область стабилизации сингулярных чисел отвечает области монотонного убывания их возмущений с ростом номера, тогда как стабилизация сингулярных векторов отвечает области, в которой их возмущения сравнимы с 90 градусами. Показано, что процесс стабилизации обусловлен математическими свойствами рассматриваемых параметров. Значимость полученного результата заключается в возможности его использования для усовершенствования различных систем защиты информации, которые построены или исследуются с применением общего подхода к анализу их состояния, как в теоретическом, так и в практическом плане. В работе приведены примеры такого использования.

Ключевые слова: система защиты информации, сингулярный вектор, сингулярное число, чувствительность, активная атака.

ВВЕДЕНИЕ

С каждым днем по мере все более широкого и глубокого внедрения информационных технологий во все сферы жизни общества, создания значительного объема конфиденциальных и критически важных данных в цифровом виде, повсеместно возрастает приоритет задач информационной безопасности, в том числе в сфере энергетической инфраструктуры [1]. Управление энергетическими системами требует разработки новых эффективных подходов, которые основываются, в частности, на современных геоинформационных технологиях, внедрение которых предполагает обязательное обеспечение безопасности данных [2]. Чтобы обеспечить безопасность локальных данных в энергетической отрасли, важно создать безопасную ИТ-среду, определить способы обмена и обработки данных, одновременно защищая их от внешних атак. Это может достигаться путем защиты самих данных, например, с помощью шифрования или использования методов стеганографии, скрывающих сам факт существования секретной информации, путем защиты каналов связи, сетей [3] и т.д. Однако организация эффективной защиты информации требует комплексного подхода, включающего в себя законодательную, программную, техническую, морально-этическую, физическую, криптографическую составляющие. В связи с этим в октябре 2024 года в ЕС вступает в силу Директива о сетевой и информационной безопасности (NIS2) [4], которая потребует от организаций в ЕС (а также тех, кто ведет бизнес с ЕС) установления конкретного базового уровня мер безопасности для снижения риска кибератак, повышения общего уровня защиты информации, комплексного подхода к ее организации. В частности, энергетический сектор для своего функционирования должен будет реализовать [4]: оценки рисков и политики безопасности для информационных систем; политику и процедуры оценки эффективности мер безопасности; политику и

процедуры использования криптографии и другие не менее важные меры.

Эффективность обеспечения защиты информации в любой области, главным образом, зависит от того теоретического базиса [5,6], в частности, математического, который положен в основу используемых методов и алгоритмов: насколько он является универсальным, насколько правильно определена область его использования, определены или оценены рекомендованные параметры, от полноты и правильности обоснования базовых положений. Огрехи в том или ином из перечисленных выше пунктов могут привести к недееспособности используемого метода в критический момент и, как следствие, к катастрофическим последствиям как для отдельного человека, фирмы, предприятия, так и для общества в целом.

Основными критериями защищенности информации являются конфиденциальность, целостность, доступность [7], однако некоторые современные ученые-теоретики готовы с этим поспорить. Так авторы [8] считают, что информационная безопасность – это сознательный или подсознательный процесс, в котором люди и организации пытаются создавать устойчиво-жизнеспособные (бизнес-) ресурсы на основе информации, не выделяя, не разграничивая и не концентрируясь на основных критериях ее защищенности. И хотя такой взгляд имеет право на существование, авторы настоящей работы с ним категорически не согласны: явно или не явно критерии защищенности информации необходимо будут учтены при разработке и функционировании любой системы защиты информации (СЗИ), что подтверждается непосредственно содержанием и выводами самой работы [8].

Важное место в общей теории информационной безопасности занимают проблемы управления, которым, в частности, посвящена работа [9], где поднимается критически актуальный на сегодняшний день вопрос «двойственности» отношений между информационными технологиями и человеком: информационные системы возникают в результате взаимно преобразующего взаимодействия между информационными технологиями и организацией; информационные системы являются результатом использования ИКТ в организации, и именно организация обеспечивает функционирование информационной системы. Авторами отмечается необходимость учета сложной связи между информационными технологиями и обществом, что не может не учитываться при организации процесса защиты информации. И хотя здесь уделено достаточное внимание основополагающим теориям предлагаемого авторами подхода, отсутствие математического фундамента не позволяет объективно оценить его универсальность, в отличие от [10,11], где адекватное использование теории чисел, матричного анализа, модулярной арифметики, линейной алгебры приводит к последовательному формированию фундаментального базиса криптографии; аналогичные вопросы решаются для организации сетевой безопасности.

Математический аппарат, используемый для обеспечения эффективного анализа угроз информационной безопасности, часто основывается на теории вероятностей, теории игр [12]. Так для исследования процессов атак на информацию в [13] используются теория дифференциальных игр и дифференциальных преобразований, теория графов, которые позволяют создать теоретические (математические) основы для моделирования указанных процессов. Работа автора по созданию общей методологии синтеза и анализа дифференциально-игровых моделей и методов моделирования процессов кибератак была продолжена в [14]. Использование современного математического базиса в разработанной методологии дало возможность для интеграции систем информационной безопасности в современные IT-технологии. Однако, как отмечается авторами [12], существующие математические подходы не устраняют в полной мере теоретические проблемы, имеющие место на сегодняшний день в информационной безопасности, в частности, в интернет-пространстве, которое рассматривается как сложная социотехническая система.

В [15] был предложен общий теоретический подход для анализа состояния и технологии функционирования информационных систем (ОПАИС), в частности СЗИ, основанный на теории матриц с использованием теории возмущений – одной из центральных математических теорий, неотделимой в своем классическом виде от асимптотических методов [16,17]. При описании любого реального процесса, как известно, можно пренебречь влиянием ряда параметров, не теряя при этом ценной информации об

основных закономерностях процесса. Здесь критически важно грамотно выделить эти параметры, чтобы иметь возможность оценить степень зависимости решения от их возмущений. Установление такой зависимости дает возможность для априорной оценки результата возмущающего воздействия, независимо от характера этого воздействия, возможность по анализу возмущений параметров определить свойства объекта, его чувствительность, а значит предвидеть реакцию объекта на конкретное возмущающее воздействие, установить достаточные условия нечувствительности объекта к возмущениям.

ОПАИС хорошо зарекомендовал себя при решении различных задач информационной безопасности [18-20]. В соответствии с данным подходом состояние/изменение состояния любой СЗИ может быть описано состоянием/возмущением сингулярных чисел (СНЧ) и сингулярных векторов (СНВ), обладающих определенными свойствами, для матрицы (матриц), которая ставится в соответствие СЗИ. При этом предполагается, что СНЧ и СНВ вычисляются при помощи нормального сингулярного разложения (НСР). Отличие НСР от обычного заключается в его единственности для матрицы, имеющей попарно различные СНЧ, за счет обеспечения дополнительного требования лексикографической положительности, накладываемого на левые СНВ [21].

Пусть F, $\overline{F}$ – это $n\times n$-матрицы исходной и возмущенной систем соответственно. Результат возмущающего воздействия (ВВ), формальным представлением которого является $n\times n$-матрица E, представляется как:

$$\overline{F} = F + E\,. \qquad (1)$$

Пусть

$$F = U\Sigma V^T \qquad (2)$$

- НСР F [21], где U, V – ортогональные матрицы, столбцы которых u_i, v_i, $i = \overline{1,n}$, являются левыми и правыми СНВ соответственно, $\Sigma = diag\left(\sigma_1(F),..., \sigma_n(F)\right)$,

$$\sigma_1(F) \ge ... \ge \sigma_n(F) \ge 0 \qquad (3)$$

– СНЧ F. Поскольку в ОПАИС оценка последствий атаки на СЗИ формально происходит в результате анализа возмущений параметров полного набора, то ключевым моментом здесь является оценка чувствительности СНЧ и СНВ к возмущающим воздействиям, которая для СНЧ соответствует формуле [22]:

$$\max_i \left|\sigma_i(F) - \sigma_i(F+E)\right| \le \|E\|_2\,, \qquad (4)$$

где $\|\cdot\|_2$ – спектральная матричная норма, из которой вытекает хорошая обусловленность СНЧ. Мерой же чувствительности к возмущающим воздействиям СНВ u_i (v_i) до сих пор считалась отделенность

$$svdgap(i,F) = \min_{i\ne j}\left|\sigma_i - \sigma_j\right| \qquad (5)$$

соответствующего СНЧ σ_i в соответствии с формулами [22]:

$$sin 2\theta_i \le 2\|E\|_2 / svdgap(i,F), \qquad (6)$$

$$sin 2\theta_i \le 2\|E\|_2 / svdgap(i,\overline{F}), \qquad (7)$$

где θ_i – угол поворота u_i (v_i) в результате возмущающего воздействия E. Однако, как уже отмечалось ранее авторами в работе, опубликованной в данном научном издании в 2022 году, формула (6) является «рабочей» только в том случае, когда ее правая часть $2\|E\|_2 / svdgap(i,F) \le 1$ (аналогично для (7)), кроме того, оценка синуса угла не дает возможности при отсутствии дополнительной информации о том, острый он или тупой, оценить сам угол.

Целью работы является развитие ОПАИС, предложенного в [15], путем детального исследования поведения параметров полного набора, определяющих матрицу СЗИ, в условиях возмущающих воздействий (активных атак) на систему.

Такое исследование даст возможность усовершенствовать существующие модели и методы, используемые в области защиты информации, перспективы чего предложены ниже.

МЕТОДЫ, РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Говоря о недостатках формул (6), (7) необходимо отметить, что их использование до настоящего момента связано не с тем, что сегодня не имеется математических выводов и результатов, которые позволят их уточнить или заменить. Дело в том, что отсутствует принципиальная возможность получения формальной априорной оценки возмущения

произвольного СНВ в результате произвольной проведенной атаки (пусть даже с учетом большего количества параметров либо с учетом параметров, отличных от используемых в (6), (7)). Поясним это на примере. Пусть первоначально

$$F = \begin{pmatrix} 1 \pm \varepsilon_1 & \pm \varepsilon_2 \\ \pm \varepsilon_3 & 1 \pm \varepsilon_4 \end{pmatrix},$$

где $\varepsilon_i > 0, i = \overline{1,4}$, незначительно отличаются от нуля. Если в результате некоторого (даже небольшого) возмущающего воздействия матрица $\overline{F}$ (1) примет вид: $\overline{F} = diag(1,1)$, то любой ненулевой вектор может рассматриваться как левый (правый) СНВ этой матрицы. Это легко видеть, учтя соответствие между сингулярным и спектральным разложениями симметричной матрицы [22], какой является $\overline{F}$. Если обозначить $\lambda_i(\overline{F})$ - собственные значения $\overline{F}$, а $\varphi_i(\overline{F})$ - ее собственные векторы ($i = 1,2$), то:

$$\sigma_i(\overline{F}) = \lambda_i(\overline{F}) = 1,$$

$$u_i(\overline{F}) = v_i(\overline{F}) = \varphi_i(\overline{F}),\ i = 1,2.$$

По определению $(\lambda_i(\overline{F}), \varphi_i(\overline{F}))$, где $\varphi_i(\overline{F}) \neq 0$, является собственной парой $\overline{F}$, если:

$$\overline{F} \cdot \varphi_i(\overline{F}) = \lambda_i(\overline{F}) \cdot \varphi_i(\overline{F}) \qquad (8)$$

В нашем случае формула (8) превращается в тождество: $\varphi_i(\overline{F}) = \varphi_i(\overline{F})$, которое имеет место для любого вектора, поэтому оценить угол поворота СНВ в результате возмущающего воздействия априори здесь принципиально невозможно. Оценка возмущения здесь будет зависеть от конкретики алгоритмической реализации процесса получения СНВ.

Заметим, что в рассмотренном примере $\overline{F}$ имеет СНЧ, кратность которого равна 2. В общем случае, если F ($\overline{F}$) будет иметь СНЧ кратные или близкие к кратным, то для соответствующего СНВ правые части (6), (7) будут стремиться к бесконечности независимо от силы возмущающего воздействия за счет стремления (равенства) к нулю отделенности (5) соответствующего СНЧ. Поэтому конкретика поведения СНВ в результате возмущающего воздействия будет зависеть не только, а в случае, когда правые части (6), (7) больше 1, то и не столько от силы и специфики этого воздействия, но и от математического (алгоритмического) способа реализации самого сингулярного разложения, не исключая особенности машинной арифметики. Заметим, что особенности машинной арифметики здесь очевидно играют важную роль. Действительно, даже незначительные в численном выражении погрешности/изменения, играют значимую роль при оценке чувствительности объекта. Процессы округлений, возникающие при вычислениях (как правило, для матриц значительных размеров), могут привести к возникновению «кратных» СНЧ даже тогда, когда на самом деле матрица не имеет таковых; и наоборот: в результате накопления вычислительной погрешности матрица, имеющая кратные СНЧ, может при вычислении «избежать» их появления.

В силу существующей взаимосвязи между СНЧ и СНВ, определяемой из формулы (2), на которую авторы уже обращали внимание в статье, опубликованной в данном научном издании в 2022 году:

$$\Sigma = U^T F V, \qquad (9)$$

$$U = FV\Sigma^{-1},\ V = F^T U \Sigma^{-1}, \qquad (10)$$

существует связь между характером возмущений СНЧ и СНВ.

Рассмотрим формулу (9) для возмущенной матрицы $\overline{F} = F + \Delta F$:

$$\begin{matrix} \overline{\Sigma} = \overline{U}^T \overline{F} \overline{V} \\ \Updownarrow \\ \Sigma + \Delta\Sigma = (U + \Delta U)^T (F + \Delta F)(V + \Delta V) \end{matrix}, \qquad (11)$$

где $\overline{\Sigma}, \overline{U}, \overline{V}$ - возмущенные матрицы СНЧ, левых и правых СНВ соответственно, а $\Delta\Sigma, \Delta U, \Delta V$ - соответствующие матрицы возмущений. Раскрывая скобки в (11) и учитывая (9), получим:

$$\begin{aligned} \Delta\Sigma = {} & \Delta U^T F V + U^T \Delta F V + \Delta U^T \Delta F V + \\ & + U^T F \Delta V + \Delta U^T F \Delta V + U^T \Delta F \Delta V + \\ & + \Delta U^T \Delta F \Delta V. \end{aligned} \qquad (12)$$

При этом все «непредсказуемости» в правой части (12), возникающие за счет неконтролируемости в поведении некоторых столбцов $\Delta U, \Delta V$, в итоге «гасятся», т.к. в левой части находится диагональная матрица $\Delta\Sigma$, диагональные элементы которой в соответствии с (4) не превосходят $\|\Delta F\|_2$. Как следует из правой части (12), это возможно лишь при значительной связи, взаимовлиянии между возмущениями левых и соответствующих правых СНВ, т.е. несмотря на то, что возмущения СНВ в случае, оговоренном выше, может быть каким угодно, но это «какое угодно» возмущение левого приводит к совершенно определенному возмущению правого СНВ и наоборот. Это подтверждается и соотношениями (10). Как показывает вычислительный эксперимент, возмущения левых и правых СНВ сравнимы как по характеру, так и по значению, при этом это наиболее сильно проявляется для СНВ, отвечающих СНЧ с наибольшими отделенностями – наибольшим СНЧ, что полностью соответствует (6), (7) (когда эти формулы в состоянии дать реальную оценку для величины возмущения СНВ). Наглядно такую связь демонстрирует рис.1, отражающий типичную картину, где очевидной является сравнимость (характера) возмущений левых и правых СНВ, при этом здесь и везде ниже возмущение Δx любого вектора x вычисляется следующим образом: $\Delta x = \|x - \bar{x}\|$, где $\bar{x}$ - возмущенный вектор x, $\|\cdot\|$ - Евклидова норма. Таким образом, ниже рассматриваются только левые СНВ, а получаемые для них результаты распространяются и на правые.

Учитывая, что любая СЗИ, как показано авторами ранее, может быть формально представлена в матричном виде, а любой цифровой контент, в частности, цифровое изображение (ЦИ), принципиально можно рассматривать как систему защиты информации (например, при организации стеганографического канала связи; при сокрытии локальных изменений контента), далее, не ограничивая общности рассуждений, для наглядности демонстрации полученных результатов используются ЦИ.

Рассмотрим более подробно характер поведения СНЧ матрицы системы в результате атаки. Хотя формула (4) констатирует нечувствительность СНЧ к возмущающим воздействиям, такая качественная оценка не дает полного представления о поведении СНЧ, говоря лишь в целом об их «адекватной» реакции на возмущение E, давая верхнюю границу их возмущений. Поскольку характер поведения СНВ зависит от поведения СНЧ в соответствии с (6), (7), (9), (10), то очевидно, что более детальная картина поведения СНЧ позволит уточнить/предвидеть характер поведения СНВ.

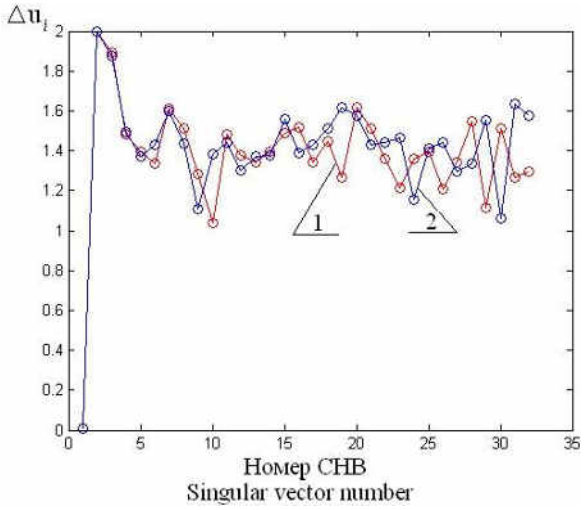


Рис.1. Графики зависимости возмущения СНВ от номера для ЦИ размером 32×32 в условиях наложения гауссовского шума с нулевым математическим ожиданием и *D*=0.0001: 1 – левые СНВ, 2 – правые СНВ[1]

Для СНЧ имеем:

- в соответствии с (3) значения СНЧ монотонно убывают, при этом как для своего первичного, так и для любого возмущенного состояния снизу СНЧ ограничены нулем;
- возмущения СНЧ при любом воздействии E не превосходит $\|E\|_2$;
- чем меньше значение СНЧ (чем больше его номер), тем меньше область его возможных возмущений. Действительно: с ростом номера СНЧ его отделенность (5), которая по сути своей определяет область, ограничивающую его возмущения, падает практически монотонно (рис.2), значения СНЧ становятся достаточно густо расположены.

Обозначим $y(\sigma_i, E) = \Delta\sigma_i$ дискретную функцию, которая каждому СНЧ σ_i ставит в соответствие его возмущение $\Delta\sigma_i$, полученное в результате воздействия E. Из всего перечисленного выше следуют выводы:

[1] Appendix 1

- начиная с некоторого номера $\bar{i}$ функция $y(\sigma_i, E)$ становятся монотонно убывающей (в смысле тренда), а вариации для возмущений СНЧ возможны лишь для начальных *i*;
- чем больше величина возмущающего воздействия $\|E\|_2$, тем скорее наступает процесс монотонного убывания возмущений СНЧ, который далее будем называть процессом *стабилизации СНЧ* (рис.3), т.к. быстрее наступает момент, когда величина возмущения СНЧ σ_i ограничена (определяется) исключительно математически - величиной самих последовательных СНЧ σ_{i-1}, σ_{i+1} (рис.4);
- при малом возмущающем воздействии следствием выводов предыдущего пункта может стать отсутствие стабилизации СНЧ. Действительно, если величина $\|E\|_2$ относительно мала, то возмущения СНЧ в силу их нечувствительности могут колебаться, не выводя возмущенные СНЧ за пределы их возможных, не нарушающих монотонности (3), значений (рис.3(e)).

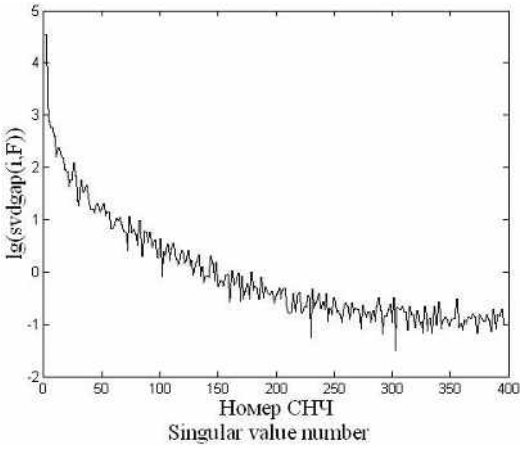


Рис.2. Иллюстрация изменения отделенности СНЧ с ростом его номера.[2]

Таким образом, возмущения СНЧ σ_i ограничивается сверху не только, а в случае значительной $\|E\|_2$ и не столько величиной нормы ВВ, но и отделенностью $svdgap(i,F)$ самого СНЧ, т.е. значениями ближайших СНЧ σ_{i-1}, σ_{i+1}; для большого ВВ именно отделенность (величина) СНЧ σ_i очень скоро начинает играть определяющую роль для величины $\Delta\sigma_i$ возмущения СНЧ, т.е. процесс стабилизации, область стабилизации обусловлены по сути именно математическими характеристиками СНЧ.

Рассмотрим теперь детально итог возмущающего воздействия на СНВ матрицы информационной системы.

Результирующее возмущение СНВ очевидно несет в себе две составляющие:

- непосредственно возмущение от возмущающего воздействия *E* на систему;
- возмущение, возникающее за счет удовлетворения требований ортогональности и лексикографической положительности СНВ при построении НСР (2).

Необходимо отметить, что вторая составляющая является чисто математической: это дополнительные возмущения, которые не обусловлены самим ВВ, а являются результатом приведения матриц *U* и *V* в (2) к требуемому сингулярным разложением виду после непосредственного ВВ.

Как только какой-то СНВ u_i в результате такого суммарного возмущения повернется на угол, близкий к 90 градусам, все, следующие за ним, которые были попарно ортогональны с ним и должны остаться таковыми в результате суммарного возмущения, будут разворачиваться на угол, близкий к 90 градусам (такой результат далее назовем *стабилизацией СНВ*), при этом некоторые СНВ могут остаться практически неизменными. Последнее происходит в силу следующих причин: как авторами настоящей работы было доказано ранее, каждый координатный ортант пространства R^n СНВ может содержать не более 1 СНВ; при повороте на 90 градусов СНВ меняет координатный ортант. При значительной размерности пространства СНВ такие изменения ортантов для большого их количества (при повороте на угол, близкий к 90 градусам) может привести к тому (в силу того, что количество координатных ортантов превосходит количество СНВ, определяемых НСР), что некоторые из СНВ останутся ортогональными (близкими к ортогональным) всем предыдущим без изменения ортанта, и вообще без значимого возмущения. Иллюстрацией сказанному может служить система трех ортогональных нормированных векторов a,b,c в пространстве R^3. При повороте векторов a и b на угол в 90 градусов так, что

[2] Appendix 1

они остались в пределах плоскости, которой они принадлежали первоначально, вектор c, оставаясь неизменным, будет сохранять попарную ортогональность с a и b. Такая ситуация возможна в конце процесса ортогонализации, для СНВ, отвечающих наименьшим СНЧ. При этом на графике зависимости возмущения СНВ от номера происходит «выброс» практически в ноль, приводя к тому, что за таким вектором картина для возмущений последующих СНВ будет аналогична картине для первых, отвечающих максимальным СНЧ (рис.5).

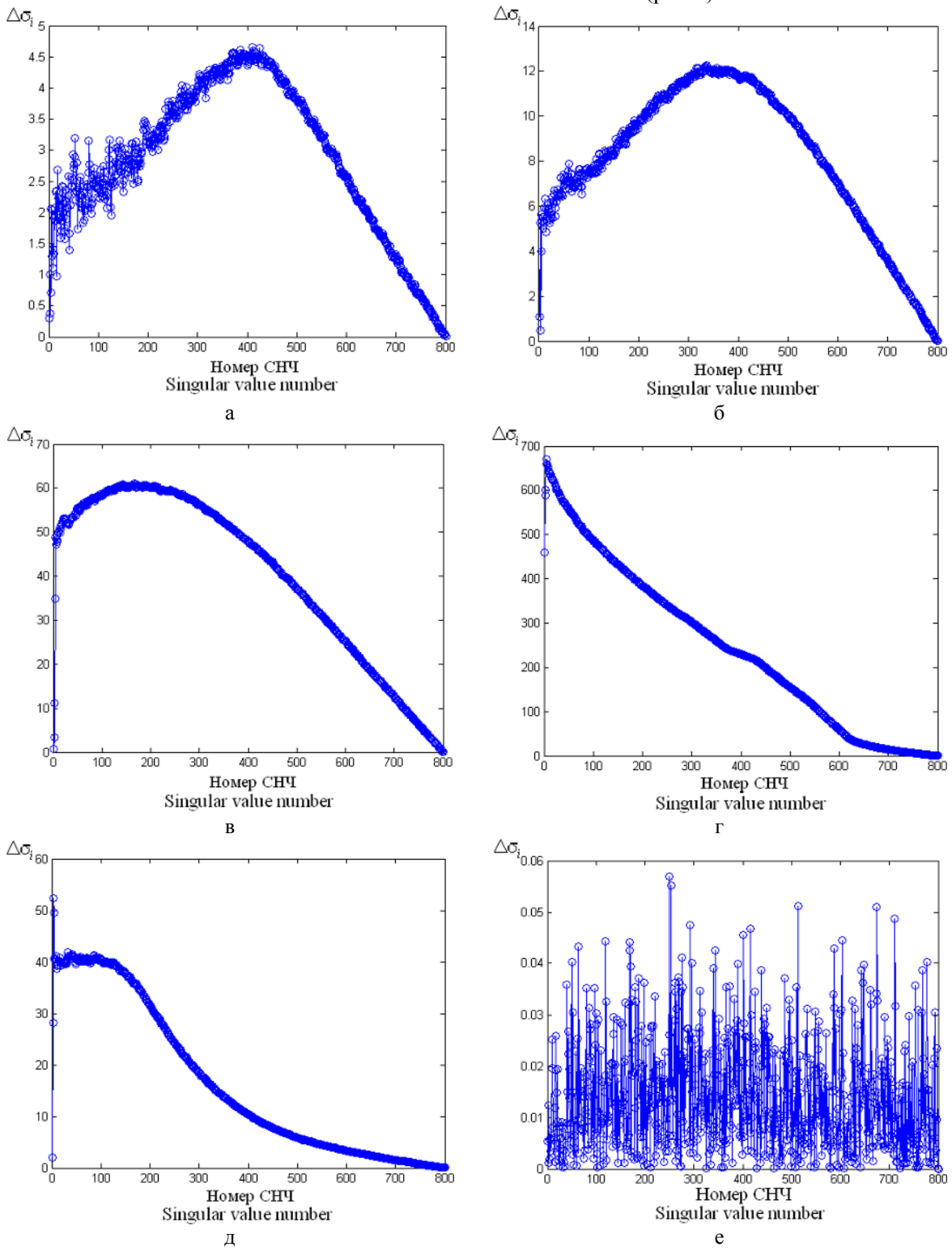


Рис.3. Графики зависимости возмущения СНЧ от его номера для конкретного ЦИ при различных возмущающих воздействиях: а –

[3] Appendix 1

мультипликативный шум, *D*=0.001 (*E*=30.5) б – гауссовский шум, *D*=0.00001 (*E*=48.3); в - гауссовский шум, *D*=0.0001 (*E*=143.6); г – шум «соль-перец», *d*=0.005 (*E*=858.9); д – усредняющий фильтр, маска 5×5 (*E*=100.8); е - гауссовский шум, *D*=0.0000003 (*E*=1.8)[3]

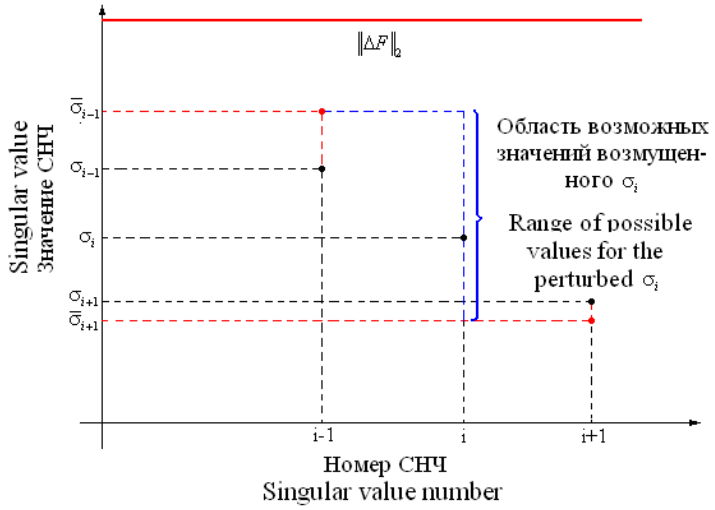


Рис.4. Графическое представление области возможных возмущений СНЧ в условиях возмущающего воздействия[4]

Для наименьших СНЧ их возмущения очень малы при любых ВВ, т.е. в абсолютном смысле наименьшие СНЧ остаются практически неизменными. Тогда возмущения СНВ, отвечающих наименьшим СНЧ, определяется математической составляющей при построении сингулярного разложения (требование ортогональности СНВ) и характер этих возмущений практически не зависит от силы и характера ВВ на систему, что полностью подтверждается результатами вычислительного эксперимента, проведенного с более чем 5000 ЦИ разного размера, формата (с потерями, без потерь), полученных профессиональными [23,24] и непрофессиональными видеокамерами, т.е. систематичность стабилизации возмущений СНВ на уровне 90 градусов для последних номеров – это результат математической составляющей сингулярного разложения. Иллюстрация последнему приведена на рис.6, где показаны возмущения СНВ под действием непосредственного возмущающего воздействия на систему и возмущения, полученные после вычисления НСР матрицы возмущенной системы, для которой, начиная с 25-го СНВ происходит стабилизация СНВ.

Процессы стабилизации (ее наступление или отсутствие) СНВ и СНЧ, учитывая (9), (10), (11), очевидно будут связаны между собой, будут определять друг друга, т.к. оба эти процессы обязаны своим появлением именно математическим особенностям рассматриваемых параметров, математическим свойствам (нормального) сингулярного разложения матрицы. Этот вывод полностью подтверждается результатами вычислительного эксперимента, демонстрирующими совпадение областей стабилизации СНЧ и СНВ, проиллюстрированными на рис.7 для одного ЦИ размером 800×800 пикселей.

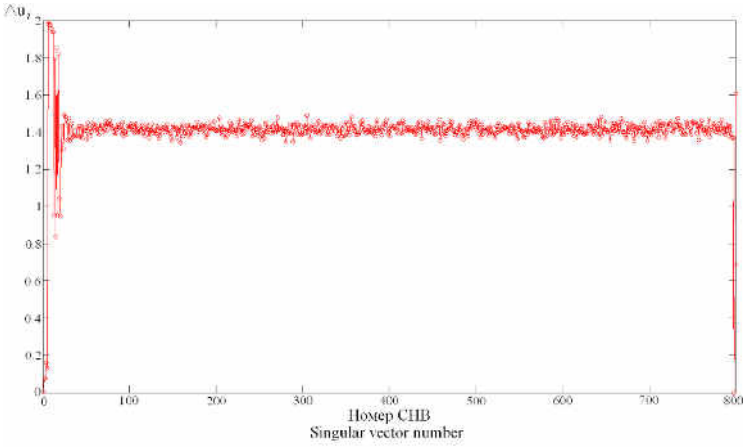
В настоящее время при обработке, анализе, исследовании матриц большого размера, каковыми являются, как правило, матрицы, отвечающие различным СЗИ, в частности ЦИ, кадрам цифрового видео, используются блочные методы, подразумевающие, что матрица контента стандартным образом разбивается на непересекающиеся блоки, которые обрабатываются последовательно/параллельно. С учетом этого в работе проведен анализ поведения СНЧ и СНВ блоков в условиях ВВ. Установлено, что для средних значений возмущений СНЧ и СНВ блоков матрицы информационного контента, характер их поведения будет аналогичным установленному выше, типичные результаты чего представлены на рис. 8 для конкретного ЦИ.

Полученные в работе результаты могут быть использованы для различных усовершенствований различных СЗИ, которые построены или исследуются, в частности с применением ОПАИС, как в теоретическом, так и в практическом плане.

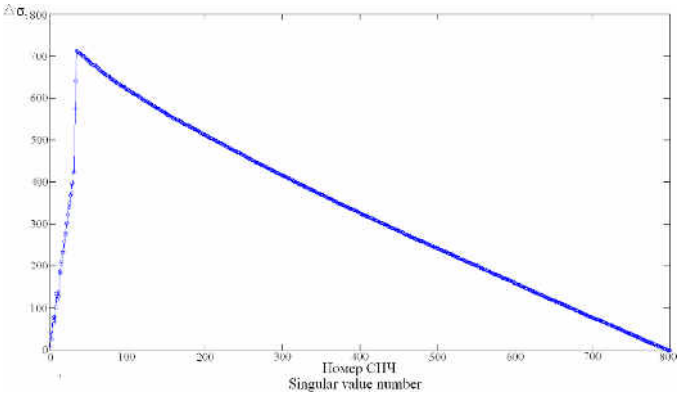
Рассмотрим лишь некоторые примеры из области стеганографии – бурно развиваю-

[4] Appendix 1

щегося сегодня направления защиты информации [25,26], представляя процесс стеганопреобразования в соответствии с (1), где F и $\overline{F}$ - матрицы контейнера и стеганосообщения (СС) соответственно.

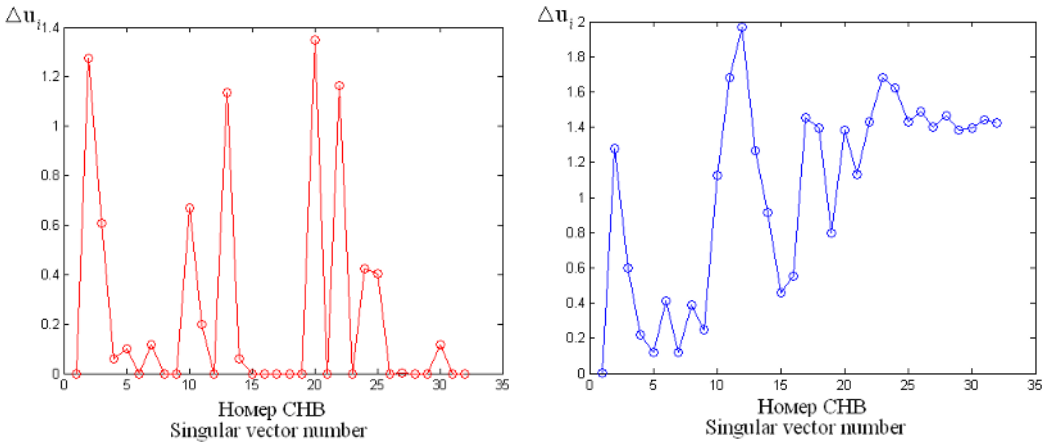


а



б

Рис.5. Графики зависимости возмущений параметров полного набора для матрицы ЦИ от номера: а – СНВ; б – СНЧ[5]



а б

Рис.6. Графики зависимости возмущения СНВ от их номера: а – реальные возмущения СНВ в результате стеганопреобразования ЦИ-контейнера стеганометодом, предложенным в [21] (размер блока 32×32); б – возмущения для СНВ, полученные в результате нормального сингулярного разложения матрицы СС.[6]

[5,6] Appendix 1

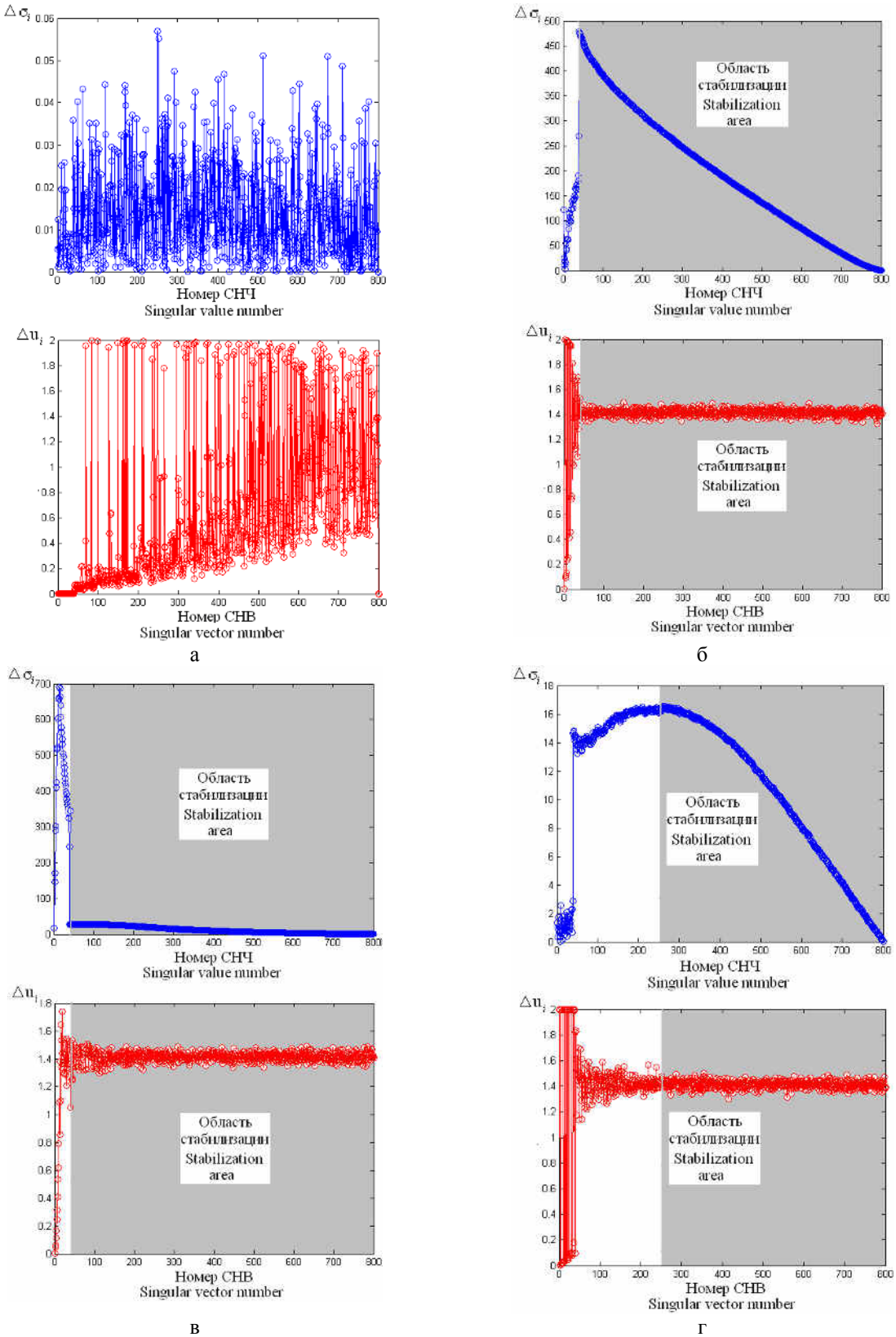


Рис.7. Соответствующие графики зависимости возмущений СНЧ/СНВ от их номера в условиях различных возмущающих воздействий: а - гауссовский шум (*D*=0.0000003); б – шум «соль-перец» (*d*=0.005); в – усредняющий фильтр (маска 5×5); г – стеганопреобразование методом LSB с пропускной способностью скрытого канала 0.5 бит/пиксель[7]

[7] Appendix 1

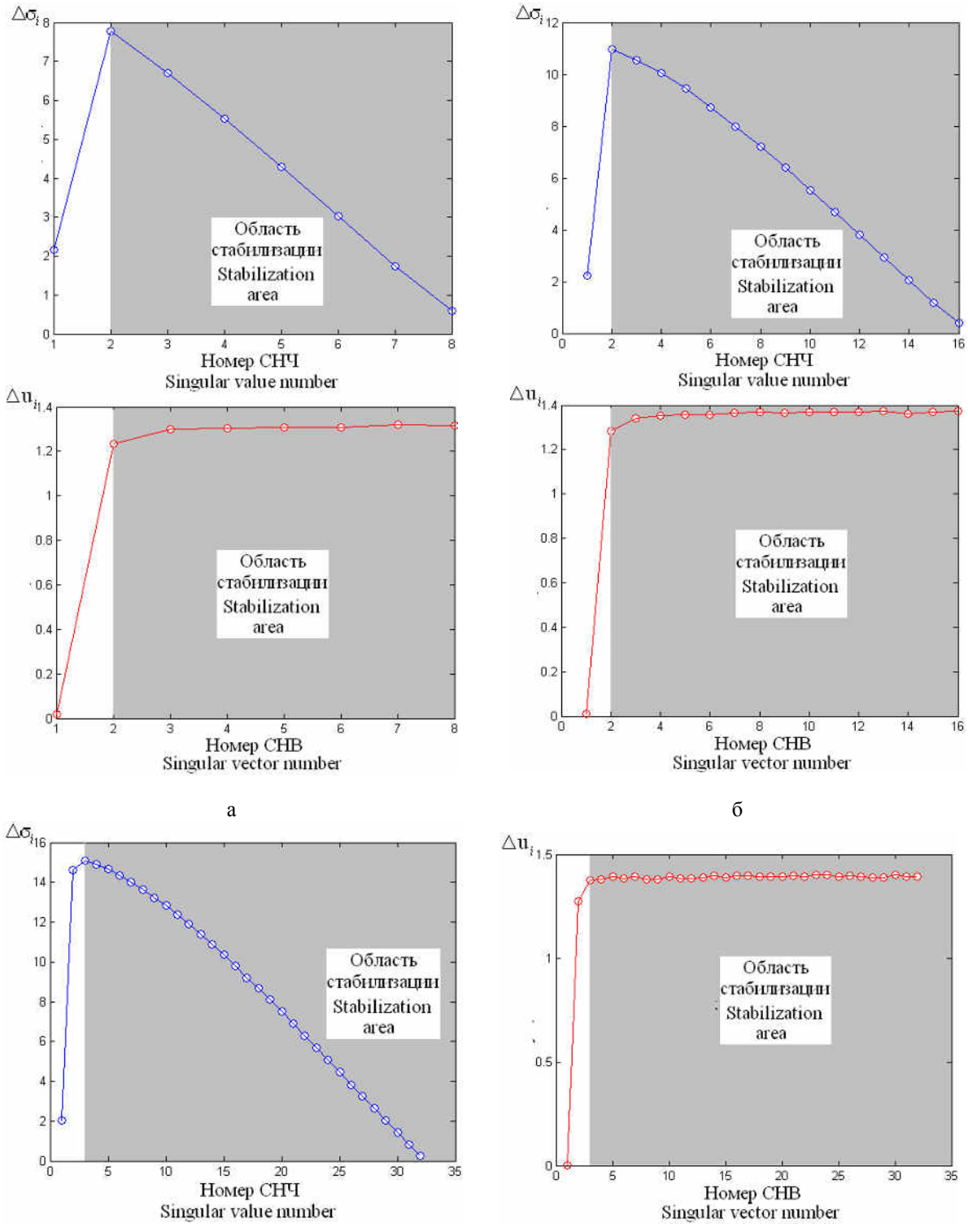


Рис.8. Соответствующие графики зависимости средних по всем *l*×*l*-блокам ЦИ возмущений СНЧ/СНВ от их номера в условиях наложения гауссовского шума с нулевым математическим ожиданием и *D*=0.0001: а – *l*=8; б – *l*=16; в – *l*=32[8]

Как установлено, СНВ, отвечающие наименьшим СНЧ, полученные в результате НСР, реагируют практически одинаково на любое ВВ, поворачиваясь на угол, близкий 90 градусам. Это дает возможность для усовершенствования составляющих процессов внедрения/декодирования дополнительной информации (ДИ) в стеганосистеме, в частности в условиях атак

[8] Appendix 1

против встроенного сообщения (АПВС), учитывая следующие факторы:

- чувствительности СНВ, начиная с некоторого номера (область стабилизации) сравнимы между собой, поэтому выбор СНВ, например, для погружения ДИ, в области стабилизации можно проводить случайным образом, делая это частью секретного ключа, повышая степень защищенности передаваемой/хранимой информации, не снижая эффективность ее декодирования;
- область стабилизации СНВ может быть определена по области стабилизации СНЧ, для чего может использоваться обычное, а не нормальное, требующее дополнительных операций для своей реализации, сингулярное разложение, определяющее однозначно СНЧ, результатом чего является уменьшение вычислительной сложности стеганометода, времени, затрачиваемого на анализ системы с использованием ОПАИС, что становится особенно актуальным в настоящий момент, когда в стеганографии все чаще используются потоковые контейнеры в режиме реального времени.

Результаты проведенных исследований позволяют провести усовершенствование в теоретическом базисе стеганографической составляющей СЗИ. Ранее авторами было получено достаточное условие нечувствительности СС к АПВС, в соответствии с которым для обеспечения нечувствительности процесс внедрения ДИ достаточно было проводить таким образом, чтобы его формальным представлением было возмущение СНВ, отвечающих СНЧ с максимальными отделенностями, а вот чувствительность СС имела место тогда, когда при погружении ДИ возмущались СНВ, отвечающие СНЧ с минимальной отделенностью. На сегодня можно утверждать, что для чувствительности СС достаточным будет возмущение СНВ, находящихся в области стабилизации, при этом непосредственное значение отделенности соответствующего СНЧ ключевой роли в этой области для чувствительности играть не будет.

Как пример усовершенствования практической реализации стеганосистемы на основе полученных в работе результатов рассмотрим стеганометод, предложенный в [21], который упоминается/используется как основа для модификации во многих работах ученых-стеганографов, где погружение ДИ происходит в левые СНВ $l\times l$-блоков матрицы ЦИ-контейнера, полученных путем ее стандартного разбиения. Целью авторов метода было обеспечение его устойчивости к АПВС. Для погружения выбиралась область матрицы U, которая не включала первый и второй столбцы и первую строку. Погружение осуществлялось путем согласования знаков соответствующего элемента матрицы U и элемента ДИ. При этом для обеспечения устойчивости метода к средним по величине ВВ, основная часть ДИ погружалась в СНВ, отвечающие значительным по величине СНЧ блоков матрицы контейнера, что принципиально могло спровоцировать возникновение артефактов на СС при значительном размере блока. Организация погружения ДИ предполагала уменьшение количество бит ДИ на 1 при переходе от u_i к u_{i+1}, доходя до нуля в случае u_l. С учетом полученных результатов можно утверждать, что с точки зрения устойчивости стеганометода к АПВС не имеет значения, в каком порядке использовать СНВ, поскольку практически одинаково будут реагировать на ВВ все СНВ в области стабилизации, а с учетом результатов, проиллюстрированных на рис.8, для наиболее распространенных размеров $l\times l$-блоков ($l\in\{4,8,16\}$) СНВ u_3, …, u_{l-1} будут находиться в области стабилизации.

Еще одним примером использования полученных результатов при практической реализации стеганосистемы может служить полученная возможность для выделения области СНЧ, наиболее предпочтительной для защиты информации от АПВС, погруженной в контейнер за счет их возмущений. Эта область включает в себя первое и последние СНЧ. Минимальность их возмущений при ВВ приведет к тому, что ДИ, внедрение которой при стеганопреобразовании вызвало их возмущение, при АПВС будет защищена в СС лучше, чем если бы ее внедрение вызвало возмущение других СНЧ в блоках контейнера, что в итоге приведет к повышению устойчивости стеганосистемы к АПВС. В настоящий момент авторы готовят к печати материалы о таком разработанном на основе метода модификации наименьшего значащего бита стеганографическом методе.

ВЫВОДЫ

В работе проведено детальное исследование поведения параметров полного набора – СНЧ и СНВ, определяющих матрицу, которая ставится в соответствие СЗИ, в условиях ВВ (активных атак), в ходе которого установлены и обоснованы особенности возмущений СНЧ и СНВ:

1. Начиная с некоторого номера функция $y(\sigma_i, E) = \Delta\sigma_i$ зависимости возмущения СНЧ от его номера становится монотонно убывающей (в смысле тренда), определяя область стабилизации СНЧ;

2. Начиная с некоторого номера возмущения СНВ находятся в окрестности 90 градусов, определяя область стабилизации СНВ;

3. Процессы стабилизации СНВ и СНЧ определяют друг друга. Оба процесса обусловлены математическими особенностями параметров, свойствами НСР матрицы, используемого для их вычисления.

Установленные свойства возмущений СНЧ и СНВ матрицы, уточняющие их чувствительность к активным атакам, дают возможность для усовершенствования различных СЗИ, которые построены или исследуются с применением ОПАИС, как в теоретическом, так и в практическом плане.

APPENDIX 1 (ПРИЛОЖЕНИЕ 1)

[1]**Fig. 1.** Dependences of the singular vectors' disturbance on the number for digital images of size 32×32 under conditions of superimposed Gaussian noise with zero mathematical expectation and D=0.0001: 1 – left singular vectors, 2 – right singular vectors

[2]**Fig. 2.** The change in the separation of singular numbers with increasing its number

[3]**Fig. 3.** Dependences of the singular number disturbance on its number for a specific digital image under various disturbing influences: a – multiplicative noise, *D*=0.001 (*E*=30.5); b – Gaussian noise, *D*=0.00001 (*E*=48.3); c – Gaussian noise, *D*=0.0001 (*E*=143.6); d – "salt-pepper" noise, *D*=0.005 (*E*=858.9); e – averaging filter, 5×5 mask (*E*=100.8); f – Gaussian noise, *D*=0.0000003 (*E*=1.8)

[4]**Fig. 4.** Graphic representation of the area of possible singular numbers' disturbances under disturbance conditions

[5]**Fig. 5.** Dependences of disturbances of the parameters of the complete set for the digital image's matrix on the number: a – singular vectors; b – singular numbers

[6]**Fig. 6.** Dependences of the singular vectors' disturbance on their number: a – real singular vectors' disturbances as a result of stegano transformation of digital image container by stegano method proposed in [21] (block size 32×32); b – disturbances of singular vectors obtained as a result of normal singular decomposition of the stegano message matrix

[7]**Fig. 7.** Corresponding dependences of singular numbers / singular vectors disturbances on their number under conditions of various disturbing influences: a – Gaussian noise (D=0.0000003); b – "salt-pepper" noise (d=0.005); c – averaging filter (mask 5×5); d – stegano transformation using the LSB method with a covert channel capacity of 0.5 bpp ?

[8]**Fig. 8.** Corresponding dependences of singular numbers / singular vectors disturbances averaged over all *l*×*l*-blocks of digital image on their number under the conditions of superimposed Gaussian noise with zero expectation and *D*=0.0001: a – *l*=8; b – *l*=16; c – *l*=32

Литература (References)

[1] Mukherjee S. Implementing Cybersecurity in the Energy Sector. Available at: https://doi.org/10.6084/m9.figshare.9728051 (accessed 15.05.2024)

[2] Hariri F., Moroz O. Possibilities of Geoinformation Systems for Implementation of the Smart Grid Concept in Electrical Distribution Networks. *Proceedings of the 2023 International Scientific and Practical Conference on Electrical Energy, Electromechanics and Technologies in Agricultural Industrial Complex*. Kharkiv, 2023. P. 101–102.

[3] Kovanen T., Nuojua V., Lehto M. Cyber Threat Landscape in Energy Sector. *Proceedings of the 13th International Conference on Cyber Warfare and Security (ICCWS 2018)*. Washington DC, USA, 2018. P. 353–361.

[4] The NIS 2 Directive. Available at: https://www.nis-2-directive.com/ (accessed 15.05.2024)

[5] Gupta M., Sharman R. *Handbook of Research on Social and Organizational Liabilities in Information Security*. IGI Global, 2009. 596 p.

[6] Awad A., Fairhurst M. *Introduction to Information Security Foundations and Applications*. IET, 2018. 416 p.

[7] Paulsen C., Byers R. Glossary of Key Information Security Terms. NIST Interagency Report 7298 Rev. 3. Available at: https://doi.org/10.6028/NIST.IR.7298r3 (accessed 15.05.2024)

[8] Horne C., Ahmad A., Maynard S. A Theory on Information Security. *Proceedings of the 2016 Australasian Conference on Information Systems*. Wollongong, 2016. P. 1–12.

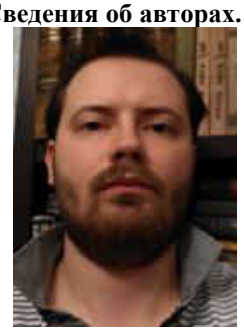
[9] Kovács L., Nemeslaki A., Orbók Á., Szabó A. Structuration Theory and Strategic Alignment in Information Security Management: Introduction of a Comprehensive Research Approach and Program. *AARMS*, 2017, vol. 16, no. 1, pp. 5–16.

[10] Forouzan B. *Cryptography and Network Security.* McGraw Hill, 2007. 721 p.

[11] Forouzan B. *Introduction to Cryptography and Network Security.* McGraw Hill, 2008. 721 p.

[12] Laracy J.R., Marlowe T. Systems Theory and Information Security: Foundations for a New Educational Approach. *Information Security Education Journal*, 2018, vol. 5, no. 2, pp. 35–48.
[13] Hryshchuk R. *Theoretical Foundations of Modeling the Processes of Attack on Information by the Methods of Theories of Differential Games and Differential Transformations*. Ruta, 2010. 280 p.
[14] Hryshchuk R., Korchenko O. Methodology of Synthesis and Analysis of Differential Game Models and Methods of Simulating Cyber Attack Processes on State Information Resources. *Ukrainian Information Security Research Journal*, 2012, no. 3, pp. 115–122.
[15] Kobozeva A., Khoroshko V. *Analiz Informatsyonnoi Bezopasnosti* [Analysis of Information Security]. Kyiv, 2009. 251 p.
[16] Kato T., Kuroda S.T. Theory of Simple Scattering and Eigenfunction Expansions. Available at: https://doi.org/10.1007/978-3-642-48272-4_5 (accessed 23.09.2022)
[17] Maslov V.P. *Asimptoticheskie Metody i Teoriya Vozmuschenii* [Asymptotic Methods and Perturbation Theory]. Moscow, 1988. 312 p.
[18] Tryfonova K., Sokalsky S. Steganoanalytical Algorithm Based on the Study of the Singular Decomposition of Digital Image Matrix Blocks. *Informatics and Mathematical Methods in Simulation*, 2022, vol. 12, no. 1-2, pp. 104–113.
[19] Kostyrka O., Melnyk M., Rudnitsky V. Steganopreobrazovanie Prostranstvennoi Oblasti i Izobrazheniya-Konteinera, Ustoichivoe k Szhatiu [Steganographic Transformation of the Spatial Domain of Cover-Image Robusted Against Compression Attacks]. *Suchasna Spetsial'na Technika – Modern Special Technics*, 2014, no. 1, pp. 75–84. (in Ukrainian)
[20] Lebedeva H. Metod Lokalizatsii i Identifikatsii Original'noi i Klonirovannoi Oblastei Izobrazheniya [Localization and Identification Method of Original and Cloned Image Areas]. *Informatyka ta Matematychni Metody v Modelyuvanni – Informatics and Mathematical Methods in Simulation*, 2014, vol. 4, no. 1, pp. 76–84. (in Ukrainian)
[21] Bergman C., Davidson J. Unitary Embedding for Data Hiding with the SVD. Available at: https://dr.lib.iastate.edu/entities/publication/bb2b5041-1c92-4ff5-b7f4-ff73c3483eed (accessed 23.09.2022)
[22] Demmel J. *Applied Numerical Linear Algebra.* SIAM, 1997. 430 p.
[23] Gloe T., Böhme R. The "Dresden Image Database" for benchmarking digital image forensics. *Proceedings of the 2010 ACM Symposium on Applied Computing (SAC '10)*. New York, 2010. P. 1585–1591.
[24] Hsu Y., Chang S. Detecting Image Splicing Using Geometry Invariants and Camera Characteristics Consistency. *Proceedings of the 2006 IEEE International Conference on Multimedia and Expo*. Toronto, 2006. P. 549–552.
[25] Mandal P.C., Mukherjee I., Paul G., Chatterji B.N. Digital Image Steganography: A Literature Survey. *Information Sciences*, 2022, vol. 609, pp. 1451–1488.
[26] Taher M.M., Ahmad A.R., Hameed R.S., Mokri S.S. A Literature Review of Various Steganography Methods. *Journal of Theoretical and Applied Information Technology*, 2022, vol. 100, no. 5, pp. 1412–1427.

Сведения об авторах.



Бобок Иван Игоревич – д.т.н., доц., Национальный университет «Одесская политехника». Область научных интересов: стеганография, стеганоанализ, социальная инженерия. E-mail: onu_metal@ukr.net

Кобозева Алла Анатольевна – д.т.н., проф., Одесский Национальный университет им. И.И. Мечникова. Область научных интересов: стеганография, стеганоанализ. Email: alla_kobozeva@ukr.net