УДК 004.4

**В.В. ХИЛЕНКО**

# ФОРМИРОВАНИЕ НОВОЙ КОНЦЕПЦИИ И ПАРАДИГМЫ ПОСТРОЕНИЯ СИСТЕМ КИБЕРБЕЗОПАСНОСТИ

**Аннотация.** Сформулированы новая концепция и парадигма построения систем кибербезопасности, адекватных угрозам несанкционированного декодирования при существующих и прогнозируемых мощностях суперкомпьютеров и нейросетей. Обоснована необходимость перехода к построению и использованию в современных условиях систем кибербезопасности, отвечающих сформулированным принципам и положениям.

**Ключевые слова:** кибербезопасность, концепция, парадигма, суперкомпьютер, нейросеть.

Существующая идеология построения систем кибербезопасности и парадигма создания соответствующих математических, технических и технологических реализаций данного класса систем сформировались более 35 лет тому назад, во время, которое можно условно назвать «досуперкомпьютерной эрой».

Публикация в 1976 г. технологии Диффи–Хеллмана [1] и появление асимметричного протокола шифрования RSA обусловили построение первых систем киберзащиты, реализующих предложенную в [1] идеологию: формирование секретного ключа (определение которого является трудоемкой задачей) без передачи его по открытому каналу связи. Полученные научно-технические результаты и потребность в повышении криптостойкости предопределили дальнейшее развитие систем киберзащиты в направлении увеличения объема вычислений, необходимых для несанкционированного декодирования информации.

Одним из наиболее известных подходов к повышению криптостойкости используемых методов шифрования является увеличение длины ключа. Соответствующие технологические изменения проводились через некоторые интервалы времени эксплуатации систем киберзащиты в определенной корреляции с увеличением производительности технических средств, предназначенных для «взлома» шифра с уточнением «за разумное время».

Другой часто используемой технологической операцией по повышению криптостойкости систем защиты электронной информации является изменение с определенным интервалом времени ключа шифрования (или самого шифра), применяемого в процессе передачи конфиденциальной информации.

Отметим, что приведенные приемы повышения криптостойкости, существенно увеличивающие объем вычислительных операций, необходимых для несанкционированного доступа к конфиденциальной информации, влияют только на количественный рост объема работы хакеров и, следовательно, должны обеспечивать увеличение времени декодирования до момента, когда передаваемая закодированная информация утратит свою ценность.

Данная логика повышения криптостойкости систем шифрования была адекватна периоду, который можно условно назвать периодом «равномерно ускоренного развития» средств вычислительной техники. Однако произошедшее в последние годы экспоненциальное ускорение в развитии производительности компьютерных систем ставит под сомнение целесообразность дальнейшего построения систем киберзащиты на основе указанных ранее подходов. Обосно-

© В.В. Хиленко, 2019

ванность такого вывода подтверждают данные о существенном ускорении в повышении мощности новых вычислительных комплексов, в частности информация о создании в Китае суперкомпьютера нового поколения «Тянхе-3» (18.05.2018), о разработке в США суперкомпьютера «Summit» для министерства энергетики (09.06.2018), о построении в Великобритании нейроморфного суперкомпьютера «SpiNNaker» (06.11.2018) и т.д.

По указанным датам публикаций информационных сообщений можно судить об ускорении, с которым происходит существенное увеличение вычислительной мощности суперкомпьютеров (вычислительных систем), а по характеристикам их производительности, измеряемым в миллиардах операций в секунду, — об улучшении условий (повышении возможностей) для несанкционированного декодирования: достижение приемлемых затрат времени на выполнение однотипных операций, в частности разложение на множители даже для очень больших чисел [2]. При сравнении [3] производительности современных суперкомпьютеров и компьютерных систем (нейросетей) с вычислительными комплексами, существовавшими во время опубликования работы Диффи и Хеллмана, становится очевидно, что сформированная ранее идеология построения систем киберзащиты не соответствует динамике изменений технических характеристик современного оборудования на рынке многопроцессорных вычислительных комплексов.

Отметим также, что в настоящее время помимо построения традиционных компьютерных систем интенсивно развивается направление создания квантовых компьютеров, появление которых может принципиально изменить ситуацию с процессом обработки больших массивов данных. По мнению ряда экспертов, реализация данного класса компьютеров обеспечит практически мгновенное решение задач дешифрования, связанных с очень большим объемом вычислений [2].

Создание квантовых компьютеров находится на стадии исследований, но приведенные данные о скорости развития уже реализованных суперкомпьютеров показывают, что наступил век сверхбыстрых суперкомпьютерных вычислений и экспоненциального повышения производительности суперкомпьютеров и требуются новые стратегии обеспечения защиты информации и новая парадигма построения систем криптозащиты.

Как отмечеалось ранее, существующая идеология киберзащиты направлена на обеспечение несоответствия времени несанкционированного дешифрования $t_{\text{hac}}$ (hacking) таким величинам, как $t_{\text{sig}}$ (significancy) — время, в течение которого данная информация сохраняет свою ценность, и $t_{\text{re}}$ (reasonable) — время, установленное легальным пользователем, в течение которого недопустимо успешное несанкционированное дешифрование (так называемое «разумное время дешифрования»). Учитываются также параметры $t_{\text{en}}$ (encryption) — время шифрования и $t_{\text{cct}}$ (cipher change time) — величина интервала времени смены шифра. При этом акцент не делается на том, чтобы каким-либо образом нарушить (сделать неустойчивым) вычислительный процесс декодирования, а основные усилия для повышения криптостойкости направляются только на увеличение трудоемкости (продолжительности) самого процесса вычислений.

Использовав приведенные обозначения для описания существующей парадигмы построения систем киберзащиты, запишем

$$t_{\text{hac}} >> t_{\text{sig}},\ t_{\text{hac}} >> t_{\text{re}},\ t_{\text{en}} << t_{\text{hac}},\quad t_{\text{cct}} << t_{\text{hac}}. \tag{1}$$

Для данной парадигмы можно определить в общем виде время вычисления значения секретного ключа $x = \text{const}$ как

$$t_{\text{en}} = q_{\text{dk}} / Q, \tag{2}$$

где величина $q_{\mathrm{dk}}$ (definitions of key) определяет объем вычислений ($q_{\mathrm{dk}} = \mathrm{const}$), необходимых для определения точного значения ключа, а $Q$ — некоторая оценка производительности используемого вычислительного комплекса, с помощью которого достигается выполнение равенства

$$\varepsilon = x_n - x = 0. \tag{3}$$

Здесь $x_n$ — результат вычисления значений секретного ключа на некотором $n$-м шаге (условное «промежуточное» значение ключа, которое в данной парадигме практически не используется).

Задача, которую необходимо решать при реализации существующей парадигмы несанкционированному пользователю для доступа к информации, требует крайне большого объема вычислений и, следовательно, бóльшего времени. Согласно этой парадигме легальный пользователь, как уже отмечалось, может увеличивать длину ключа или изменять какие-либо иные параметры кодирования, увеличивая тем самым (потенциально до бесконечности) время, необходимое для несанкционированного декодирования. Аналогично, увеличивая частоту изменения ключа или шифра, система киберзащиты также делает нереальным несанкционированное дешифрование за время, в течение которого расшифровка представляет опасность для легальных пользователей (например, при проведении банковской транзакции, когда по завершении банковской операции значимость защиты информации существенно снижается либо информация становится неактуальной). При этом технология несанкционированного декодирования с помощью подбора ключа («взлома» шифра), т.е. рутинного перебора вариантов расшифровки, не представляет интерес, поскольку требует еще бóльших и практически нереальных затрат времени.

В существующей парадигме построения систем киберзащиты неявно предполагался паритет мощности вычислительных средств, используемых всеми (авторизованными и неавторизованными) участниками процесса. Но кардинальные изменения, произошедшие и происходящие на рынке средств вычислительной техники, требуют адекватных изменений в принципах и идеологии построения систем защиты информации.

В настоящее время ни одна из систем киберзащиты, построенная в соответствии с существующей парадигмой (1)–(3), не защищает пользователя от взлома с помощью миллиардных переборов шифра или многократного выполнения рутинных операций поиска искомых значений (например, вычисления, связанные с решением задачи факторизации), которые могут проводиться суперкомпьютером или вычислительным кластером (нейросетью) в автоматическом режиме.

Анализ парадигмы (1)–(3) показывает, что возникла потребность в соответствующих технологиях, обеспечивающих защиту, адекватную современному уровню техники и развиваемым аппаратным решениям, которые можно использовать для дешифрования при наличии у несанкционированного пользователя новейших суперкомпьютерных систем высокой производительности. Современные системы киберзащиты необходимо строить с учетом того, что мощности этих вычислительных комплексов (нейросетей) позволяют решать ранее нерешаемые задачи и, следовательно, делают возможными способы взлома, которые в «досуперкомпьютерную эру» были невозможны.

Новая идеология построения систем киберзащиты должна быть основана не на концепции загрузки компьютеров хакеров огромным объемом вычислений, а на концепции «обеспечения неэффективности суперкомпьютера», т.е. на применении такой технологии кодирования, при которой суперкомпьютер, используемый как средство подбора или вычисления шифра, не обеспечит декодирования информации, как бы его мощность не соотносилась с объемом необходимых вычислений.

Примером критичности рассматриваемых ситуаций, когда система киберзащиты построена согласно парадигме (1)–(3), является защита данных при проведении банковских операций. В этом случае целенаправленное объединение мощностей ряда суперкомпьютеров (многопроцессорных вычислительных комплексов с параллельной обработкой информации, нейросетей) теоретически позволяет осуществить дешифрование за время, достаточное для вмешательства в сеанс связи, что может привести к существенно негативным последствиям. При этом необходимый уровень безопасности теоретически не гарантируется ни увеличением длины ключей, ни другими множественными процедурами, имеющими количественный характер и усложняющими дешифрование.

Решить данную проблему можно, разработав механизм защиты, обеспечивающий неэффективность многократного выполнения рутинных вычислительных операций и методик подбора шифра при использовании несанкционированным пользователем многопроцессорных вычислительных комплексов и суперкомпьютеров, которые должны вскрыть этот ключ. Аналогом является работа механической системы, где движение шестеренок обеспечивает требуемый результат. Для систем передачи данных по логике процесса несанкционированного декодирования это соответствует подбору с помощью суперкомпьютера секретного ключа, необходимого для раскрытия информации в автоматическом режиме. Попадание песка или специальных добавок приводит к неработоспособности механической системы, а в рассматриваемом случае IT-систем неэффективность системы взлома ключа с помощью суперкомпьютера достигается применением проблемно-ориентированных технологий шифрования, использующих специализированный математический аппарат.

С учетом изложенного парадигму построения систем киберзащиты «суперкомпьютерной эры» можно представить в виде неравенств (1) и преобразованных соотношений (2), (3), которые запишем как

$$x \in [x_{\min}, x_{\max}],\ t_{\text{en}} = q_{\text{dk}}(\varepsilon)/Q; \tag{4}$$

$$q_{\text{dk}} = q_{\text{dk}}(\varepsilon),\ \varepsilon \le \varepsilon_{\lim}, \tag{5}$$

где $x_{\min}$ — минимальная величина диапазона значений секретного ключа, при котором легальный пользователь может проводить декодирование корректно, $x_{\max}$ — верхняя граница диапазона значений секретного ключа, $\varepsilon_{\lim}$ — предельно допустимая величина отклонения в значении секретного ключа, позволяющая правильно дешифровать закодированную информацию. Параметры $x_{\min}$, $x_{\max}$ и $\varepsilon_{\lim}$ задаются участниками сеанса связи.

Системы защиты информации, построенные в соответствии с парадигмой (1), (4), (5), обеспечат защиту авторизованных (легальных) участников сеанса связи от несанкционированного декодирования, осуществляемого в соответствии с упомянутыми суперкомпьютерными технологиями. Математические процедуры и технологии шифрования, реализующие парадигму (1), (4), (5), должны выполнять функцию песка, обеспечивающего неработоспособность процесса декодирования, осуществляемого с помощью выполнения суперкомпьютером переборов возможных значений ключа или рутинных вычислительных операций для поиска значения секретного ключа.

Математический аппарат и математические методы, обеспечивающие реализацию парадигмы (1), (4), (5), определяются при построении системы киберзащиты. Возможное решение реализации парадигмы (1), (4), (5) представлено в [4–6]. Одним из элементов этой реализации, отражающим идеологию ее создания, является алгоритм определения собственных чисел матриц [7] на основе теоремы Khilenko [8], когда итерационными процедурами достигается приемлемое значение $\lambda_n$, а объем вычислений не растет экспоненциально при увеличении числа $n$ — размерности матрицы.

Прогнозируемое дальнейшее развитие производительности суперкомпьютерной техники требует усовершенствования существующих и создания новых решений реализации парадигмы (1), (4), (5), связанных с использованием все более сложного и проблемно-ориентированного математического и программно-алгоритмического обеспечения.

Сравнивая парадигмы (1)–(3) и (1), (4), (5), можно отметить следующее.

В соответствии с парадигмой (1)–(3) несанкционированному пользователю необходимо выполнять чрезвычайно большой, но определенный объем вычислений, что при существующих неспециализированных средствах вычислительной техники требует огромных затрат времени. Процесс шифрования организован так, что рутинное многократное выполнение последовательности однотипных операций в принципе позволяет осуществлять декодирование. Следовательно, имея вычислительную систему очень большой мощности, можно быстро выполнить несанкционированное декодирование. Уверенность в защищенности информации основывается на том, что несанкционированный пользователь не располагает вычислительными средствами сверхбольшой мощности.

Согласно парадигме (1), (4), (5) несанкционированному пользователю также необходимо выполнять очень большой объем вычислений, но при этом система шифрования строится таким образом, что в процессе решения им вычислительных задач дешифрования, в том числе механического перебора возможных искомых комбинаций, на определенном этапе работы запрограммирован сбой вычислительного процесса. Тем самым закодированная информация защищается от взлома, реализуемого переборами возможных шифров, или от нахождения искомого ключа в результате многократного выполнения однотипных операций даже в случае, когда у несанкционированного пользователя имеется вычислительная техника сверхбольшой мощности.

Отметим различие концепций реализации обеих рассматриваемых парадигм. В концепции, соответствующей парадигме (1)–(3), повышение характеристик систем криптозащиты достигается увеличением объема требуемых для взлома вычислений за счет увеличения длины ключа, периодической смены шифра или других технологических операций.

В концепции, соответствующей парадигме (1), (4), (5), увеличение объема вычислений при несанкционированном декодировании достигается не за счет увеличения трудоемкости выбранной при шифровании задачи (например, задачи факторизации), а использованием специальных математических приемов, обеспечивающих необходимость многократного решения совокупности трудоемких вычислительных задач. При этом процесс дешифрования предполагает последовательное (цепочное) решение указанных взаимосвязанных задач, когда результаты решения одной задачи являются исходными данными для последующей. Ошибки в решении любой предыдущей задачи обусловят некорректное решение последующих задач, что гарантирует сбой всего процесса поиска решения независимо от вычислительной мощности, используемой для несанкционированного декодирования. Концептуальным приемом повышения криптозащищенности при реализации парадигмы (1), (4), (5), принципиально отсутствующим в парадигме (1)–(3), является также повышение «чувствительности» системы киберзащиты к появлению ошибочных результатов на промежуточных этапах вычисления.

Стратегическая цель и парадигмы (1)–(3) и (1), (4), (5) совпадают: не допустить несанкционированного декодирования информации в некотором определенном интервале времени. Однако в парадигме (1), (4), (5) акцент делается не на увеличение времени, необходимого для взлома ключа, за счет возрастания объема вычислений у несанкционированного пользователя, а на гарантиро-

ванное обеспечение сбоев при выполнении вычислений, связанных с несанкционированным декодированием. При этом реализация парадигмы (1), (4), (5) не исключает возможности построения систем кибербезопасности в соответствии с парадигмой (1)–(3), позволяя их использовать как элементы, только усиливающие реализацию парадигмы (1), (4), (5). С этой точки зрения парадигма (1), (4), (5) является обобщающим решением, включающим парадигму (1)–(3) в качестве внутреннего элемента своей реализации.

СПИСОК ЛИТЕРАТУРЫ


1. Diffie W., Hellman M. New directions in cryptography. *IEEE Transactions on Information. Theory*. 1976. Vol. 22, Iss. 6. P. 644–654. DOI:10.1109/TIT.1976.1055638.
2. Мелков Ю. Квантовые компьютеры и квантовый интернет. 2017. URL: https://itc.ua/articles/kvantovyie-kompyuteryi-i-kvantovyiy-internet-segodnya-i-zavtra/.
3. Казакова И.А. История вычислительной техники: учебное пособие. Пенза: Изд-во ПГУ, 2011. 232 с.
4. Khylenko V.V. System for transmitting encoded information. PCT /UA2017/000021. 07.09.2018. Pub. No. WO/2018/160155.
5. Khylenko V.V. System for transmitting encoded information. PCT /UA2016/000064. 31.08.2017. Pub. No. WO/2017/146669.
6. Khylenko V.V. Mobile device for receiving, transmitting, and processing information and keyboard for said device. PCT/UA2016/000123. 03.05.2018. Pub. No. WO/2018/080414.
7. Grishchenko A.Z., Khilenko V.V. Determining the number of fast and slow components in decomposition of arbitrarily large linear dynamical models. *Cybernetics and Systems Analysis*. 1991. Vol. 27, N 6. P. 795–801.
8. Khilenko V.V., Strzelecki R., Kotuliak I. Solving the problem of dynamic adaptability of artificial intelligence systems that control dynamic technical objects. *Cybernetics and Systems Analysis.* 2018. Vol. 54, N 6. P. 867–873.


*Надійшла до редакції 26.12.2018*

**В.В. Хиленко**

**ФОРМУВАННЯ НОВОЇ КОНЦЕПЦІЇ ТА ПАРАДИГМИ ПОБУДОВИ СИСТЕМИ КІБЕРБЕЗПЕКИ**

**Анотація.** Сформульовано нову концепцію і парадигму побудови систем кібербезпеки, адекватних загрозам несанкціонованого декодування для наявних і прогнозованих потужностей суперкомп'ютерів і нейромереж. Обґрунтовано необхідність переходу до побудови та використання в сучасних умовах систем кібербезпеки, що відповідають сформульованим принципам і положенням.

**Ключові слова:** кібербезпека, концепція, парадигма, суперкомп'ютер, нейромережа.

**V.V. Khilenko**

**CREATING A NEW CONCEPT AND PARADIGM FOR BUILDING CYBERSECURITY SYSTEMS**

**Abstract.** A new concept and paradigm of building cybersecurity systems adequate to the threats of unauthorized decoding with the available and predicted capacities of supercomputers and neural networks has been formulated. The necessity of the transition to the construction and use in modern conditions of cyber security systems that meet the formulated principles and provisions is substantiated.

**Keywords:** cybersecurity, concept, paradigm, supercomputer, neural network.

**Хиленко Владимир Васильевич,**
доктор техн. наук, профессор, профессор кафедры Национального университета биоресурсов и природопользования Украины МОН Украины, Киев, e-mail: vkhilenko@ukr.net.