ISSN 2073-2600

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

3

(138)

Подписывайтесь,
читайте,
пишите в наш журнал

Москва 2022

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

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

Межотраслевой научно-технический журнал

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

Подписной индекс **79379**

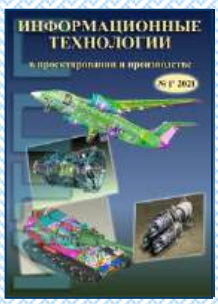
Издается с 1984 года

Межотраслевой научно-технический журнал

Конструкции из композиционных материалов
(4 выпуска)

Подписной индекс **80089**

Издается с 1981 года



Научно-технический журнал

Информационные технологии в проектировании и производстве
(4 выпуска)

Подписной индекс **79378**

Издается с 1976 года

Межотраслевой научно-практический журнал

Экология промышленного производства
(4 выпуска)

Подписной индекс **80090**

Издается с 1993 года

Научно-практический журнал

Вопросы защиты информации
(4 выпуска)

Подписной индекс **79187**

Издается с 1974 года

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

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

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

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

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

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

3 (138)

Москва 2022
Основан в 1974 г.

С О Д Е Р Ж А Н И Е

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Инженерная криптография

Управление доступом

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

Учредитель *Федеральное государственное унитарное предприятие «Научно-технический центр оборонного комплекса «Компас»*

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ИНЖЕНЕРНАЯ КРИПТОГРАФИЯ

УДК 004.315.2
DOI: 10.52190/2073-2600_2022_3_3
EDN: VHFDRD

Структура устройства шифрования алгоритма Магма с обеспечением надежности вычислений и защиты от утечки по побочным каналам

[1] *А. А. Бахтин*, канд. техн. наук; [1] *Е. А. Бордашевич*; [1] *Е. М. Зверев*;
[2] *И. Е. Любушкина*, канд. техн. наук; [1] *А. В. Шарамок*, канд. техн. наук
[1] Национальный исследовательский университет «МИЭТ», г. Зеленоград, Москва, Россия
[2] ООО Фирма «АНКАД», Москва, Россия

Приведено описание структуры устройства, реализующего криптографическую обработку данных в соответствии с алгоритмом Магма с защитой от утечки информации по каналам ПЭМИН и повышение достоверности криптографических вычислений. Защита от утечки информации по каналам ПЭМИН обеспечивается созданием оптимальной маскирующей помехи в криптографическом устройстве. Оптимальная маскирующая помеха создается путем одновременной синхронной обработки данных в соответствии с алгоритмом Магма в прямом представлении и в инвертированном представлении. Повышение надежности криптографических вычислений достигается благодаря тому, что в устройстве криптографической защиты информации одновременно обрабатывают данные в соответствии с алгоритмом Магма в прямом представлении и в инвертированном представлении с последующим сравнением результатов обработки в прямом и инверсном представлении между собой. Предложенная структура блока итерации шифрования позволяет введением внешнего однобитового признака переключать устройство итерации шифрования на работу с данными в прямом или инвертированном представлении.

Ключевые слова: криптографическое устройство, алгоритм шифрования Магма, побочные каналы, шифрование, надежность.

Разработка устройств криптографической защиты информации, обеспечивающих высокий уровень защищенности, требует решения ряда специфических задач [1], таких как обеспечение надлежащего уровня криптографических, инженерно-криптографических и специальных свойств разрабатываемых устройств. Обеспечение криптографических свойств (мера надежности защиты зашифрованной информации, представляющая собой трудоемкость, измеренную в количестве элементарных операций, которые необходимо выполнить для осуществления эффективного криптоанализа) относительно широко освещено в современной технической литературе, например, в материалах Технического комитета по стандартизации ТК-26 [2]. В отношении обеспечения инженерно-криптографических свойств (способность криптографического преобразования к эффективной реализации в устройствах шифрования с обеспечением криптостойкости при учете реальных

Бахтин Александр Александрович, заведующий кафедрой "Телекоммуникационные системы".
E-mail: bah@miee.ru
Бордашевич Екатерина Алексеевна, студент магистратуры.
E-mail: ekaterina.bordashevich@yandex.ru
Зверев Евгений Михайлович, старший преподаватель.
E-mail: emzverev@mail.ru
Любушкина Ирина Евгеньевна, главный специалист.
E-mail: grehneva@mail.ru
Шарамок Александр Владимирович, доцент.
E-mail: sharamok@mail.ru

Статья поступила в редакцию 2 сентября 2022 г.

инженерных свойств аппаратуры) и специальных свойств (способность противостоять утечкам опасной информации по возможным побочным каналам при реализации криптографического преобразования в устройстве шифрования) существуют только отдельные публикации [1, 3, 4].

В настоящей статье изложены предложения авторов по общей структуре устройства криптографической защиты информации, реализующего криптографическое преобразование в соответствии с алгоритмом "Магма" по стандарту ГОСТ Р 34.12-2015 [5]. При этом рассматриваются два аспекта обеспечения инженерных и специальных свойств: обеспечение надежности криптографических вычислений и защита от утечек информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

На основании ранее полученных авторами результатов по формированию оптимальной маскирующей помехи [6] и инверсной арифметике для алгоритма "Магма" [1, 7] авторы предлагают структуру устройства криптографической защиты информации, обеспечивающего защиту от утечки информации по каналам ПЭМИН и одновременное повышение надежности криптографических вычислений.

Постановка задачи

Одним из основных способов повышения надежности криптографических средств является дублированное выполнение криптографических преобразований [1]. Например, при реализации криптографических средств программным способом используются различные варианты временного дублирования, повторных просчетов одних и тех же преобразований с последующим сравнением результатов. В этом случае возможно обнаружение сбоев, происходящих в процессе вычислений. Если сбои носят систематический характер, то подобные дублирования не позволяют их обнаружить и необходимо использовать дополнительные механизмы, например, такие, как самоблокируемый оператор сравнения [1].

При аппаратной реализации криптографических средств возможности по повышению надежности криптографических вычислений существенно расширяются. Необходимо отметить, что аппаратная реализация криптографических средств не всегда оправдана, так как несет существенные дополнительные издержки и усложняет информационную систему в целом. В то же время аппаратная реализация является приоритетной для обеспечения требуемого уровня защищённости в устройствах, применяемых для обработки информации высокой важности. Это требуется не только с точки зрения аспектов, рассматриваемых в данном исследовании, но и по другим, значительно более широким причинам, рассмотрение которых выходит за рамки настоящего исследования.

Основным методом обеспечения надежности криптографических вычислений в криптографических устройствах является аппаратное дублирование вычислений [1, 8]. Типовая структура криптографического устройства [4, 8] с аппаратным дублированием представлена на рис. 1.

Основными блоками в составе криптографического устройства являются основной и дублирующий блоки шифрования данных, блок управления процессом шифрования, интерфейс открытых данных, интерфейс шифрованных данных, блок сравнения результатов шифрования и блокировки, блок синхронизации. Блоки взаимодействия с внешним интерфейсом и сравнения результатов шифрования могут быть объединены в единый блок, например, в рамках одной интегральной схемы. В структуре криптографического устройства, предлагаемого авторами, важную роль играет блок синхронизации, так как он важен для решения задачи защиты от утечек информации по каналам ПЭМИН.

В случае реализации устройства шифрования с одним входным/выходным интерфейсом типовая структура изменится за счет объединения двух интерфейсов в один и перевода схемы сравнения на внешний интерфейс.

Если рассматривать устройство основного и дублирующего блоков шифрования, то, как правило, они имеют идентичную структуру. Например, известно устройство шифрования данных (рис. 2), описанное в патенте РФ [4].

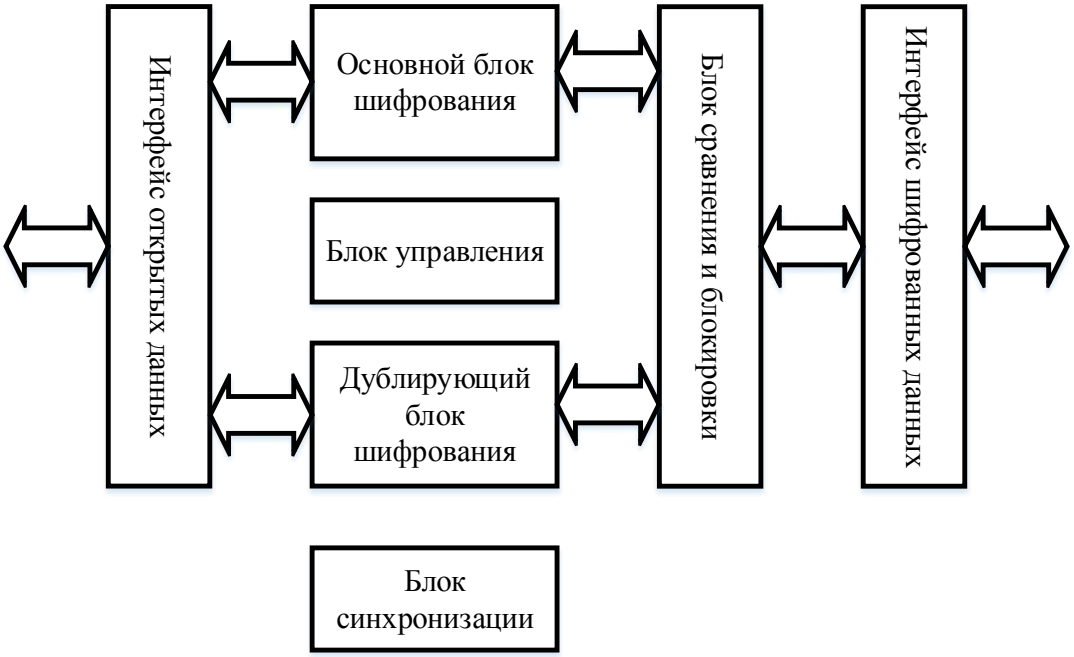


Рис. 1. Типовая структура проходного шифратора

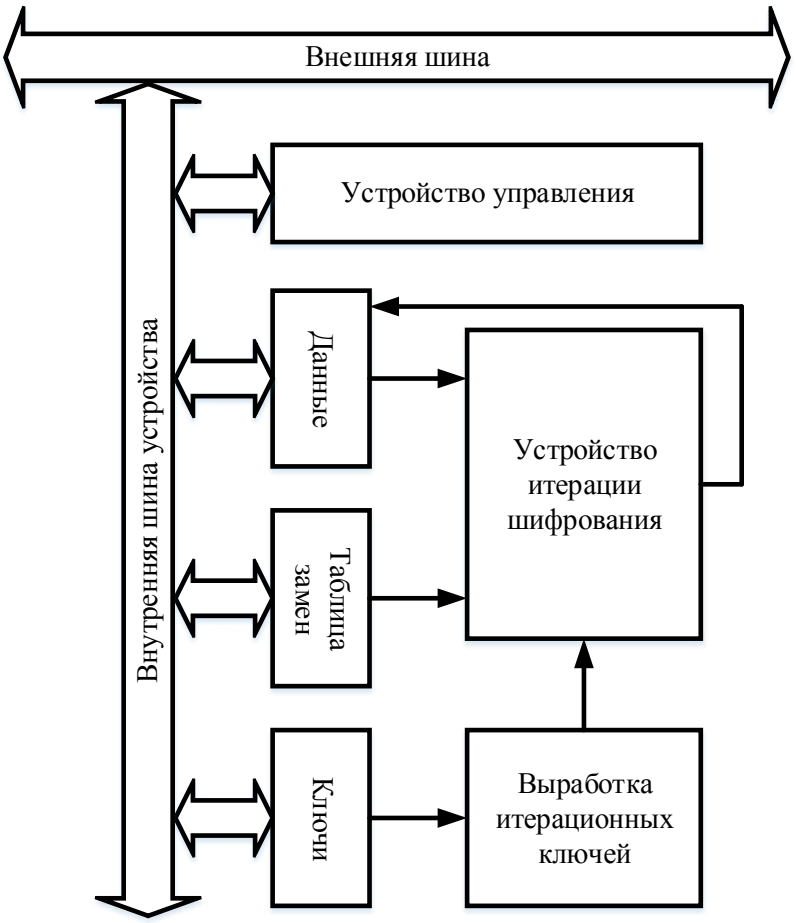


Рис. 2. Структура блока шифрования

В этом изобретении техническим результатом является повышение тактовой частоты устройства шифрования данных. Известно, что противодействовать съему опасной информации по побочным каналам возможно путем создания оптимальной маскирующей помехи [6]. При этом оптимальная маскирующая помеха создается при обработке данных в инвертированном представлении [6, 7]. При криптографическом преобразовании данных в соответствии с алгоритмом "Магма" по стандарту ГОСТ Р 34.12-2015 для создания оптимальной маскирующей помехи в устройстве одновременно с преобразованием данных с прямым представлением необходимо реализовать синхронную обработку данных в инвертированном представлении.

Из приведенной на рис. 1 структуры можно сделать вывод, что традиционная структура аппаратных криптографических устройств не противоречит изложенным в [6, 7] принципам и в ней могут быть одновременно реализованы обработка информации в прямом и инверсном представлении, что обеспечит защиту от утечки информации по каналам ПЭМИН [6] и одновременно обеспечит повышение надежности при криптографических вычислениях в соответствии с классическими принципами разработки криптографических устройств [1].

Таким образом, задачей настоящего исследования является описание структуры устройства, реализующего криптографическую обработку данных в соответствии с алгоритмом "Магма" с защитой от утечки информации по каналам ПЭМИН и обеспечением достоверности криптографических вычислений.

Защита от утечки информации по каналам ПЭМИН обеспечивается благодаря созданию оптимальной маскирующей помехи в криптографическом устройстве. Оптимальная маскирующая помеха создается путем одновременной синхронной обработки данных в соответствии с алгоритмом Магма в прямом представлении и в инвертированном представлении [6].

Повышение надежности криптографических вычислений достигается благодаря тому, что в устройстве криптографической защиты информации одновременно обрабатываются данные в соответствии с алгоритмом Магма в прямом представлении и в инвертированном представлении с последующим сравнением результатов обработки в прямом и инвертированном представлении между собой.

Реализация вычислений в прямом и инвертированном представлении

Результаты работ [1, 7] показывают, что решить поставленную задачу возможно путем использования двух идентичных схемотехнических блоков, один из которых обрабатывает данные в соответствии с алгоритмом Магма в прямом представлении, другой — в инвертированном представлении.

Возможность обработки данных в прямом и инвертированном представлении идентичными схемотехническими блоками обусловлена следующими свойствами алгоритма Магма [1, 5, 7].

1. Суммирование подблока данных с итерационным ключом [5] в прямом и инвертированном представлении отличается только дополнительным сложением с константой, равной единице в младшем разряде сумматора, что обеспечивает выполнение условий инвертированного сложения по модулю $2^n : \left|\bar{a} + \bar{b} + 1\right|_{2^n} = \left|\overline{a+b}\right|_{2^n}$ [1, 7]. Эта константа используется как признак обработки в прямом или инвертированном представлении (ноль — обработка в прямом представлении, единица — обработка в инвертированном представлении).

2. Подстановка по таблице замен осуществляется в соответствии с загруженной таблицей замен. При обработке данных в прямом представлении используют таблицу замен для прямого представления данных [5], при обработке данных в инвертированном представлении используют таблицу замен для инвертированного представления данных [7].

3. В блоке циклического сдвига и блоке сложения по модулю 2 операции с инвертированными данными осуществляются аналогично операциям с данными в прямом представлении.

Таким образом, блок криптографического преобразования данных в соответствии с алгоритмом Магма, обеспечивающий возможность обработки данных в прямом и инвертированном представлении, отличается от блока, обеспечивающего возможность обработки данных только в прямом представлении, наличием дополнительного входа размером в один бит. Этот дополнительный вход используется как признак обработки в прямом или инвертированном представлении.

Необходимо отметить, что исходя из структуры, представленной на рис. 2, дополнительный вход необходим не на весь блок шифрования, а только на блок итерации шифрования, так как именно в нем используется введённый признак обработки. Рассмотрим структуру блока итерации шифрования.

Реализация блока итерации шифрования

Блок итерации шифрования данных алгоритма Магма (рис. 3) состоит из блока сложения по модулю 2^{32} данных с итерационным ключом, блока подстановки по таблице замен, блока циклического сдвига, блока сложения по модулю 2.

В отношении приведённой на рис. 3 структуры возможны различные оптимизационные улучшения, например, предложенные в [9, 11]. Но в целом, структура блока итерации шифрования будет сохраняться, в части нас интересующей — возможности обработки данных в прямом и инвертированном представлении.

Для реализации возможности подобной обработки блок итерации имеет два входа (на рис. 3 обозначены 1 и 2), на которые подают 32 битные подблоки данных, подлежащих шифрованию, вход для записи в блок итерации шифрования таблицы замен (обозначен 3) и вход на который подают итерационный ключ шифрования (обозначен 4). По сравнению с устройствами, обрабатывающими данные только в прямом представлении, блок итерации шифровании имеет пятый вход, на который подают значение бита прямой или инвертированной обработки.

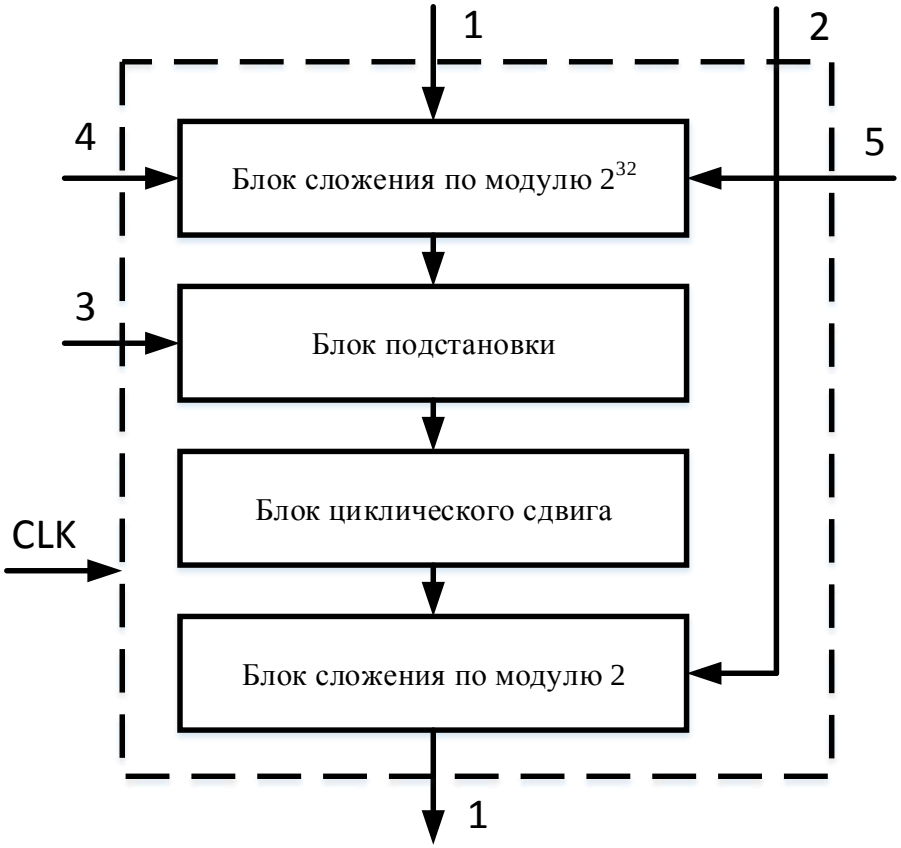


Рис. 3. Структура блока итерации шифрования

При подаче бита прямой или инвертированной обработки, равного нулю, обработку осуществляют в прямом виде, при подаче бита прямой или инвертированной обработки, равного единице, обработка осуществляется в инвертированном виде. Результат обработки итерации шифрования выдают на выход. Внутренние связи блока итерации шифрования представлены на рис. 3.

Внутри блока итерации шифрования в соответствии с алгоритмом Магма [5] данные проходят последовательную обработку от блока сложения по модулю 2^{32} до блока сложения по модулю 2. Необходимо отметить, что блок сложения по модулю 2^{32} функционирует как обыкновенный сумматор, принимающий значение переноса из старшего разряда "младшего" полного полусумматора [12]. В качестве этого значения переноса используется признак работы в прямом или инвертированном представлении данных, который поступает в блок итерации шифрования с пятого входа блока итерации шифрования. При этом, в зависимости от представления обрабатываемых данных (прямое или инвертированное), на третий вход подают таблицу замен в прямом или инвертированном представлении [5, 7]. Работа всего устройства тактируется от внешнего устройства тактового сигнала.

Реализация устройства шифрования

Изложенная выше структура блока итерации шифрования позволяет создать устройство шифрования, реализующее защиту от утечки информации по каналам ПЭМИН путем создания оптимальной маскирующей помехи за счет одновременной синхронной обработки данных в соответствии с алгоритмом Магма в прямом представлении и в инвертированном представлении и обеспечивающее надежность криптографических вычислений, в соответствии с типовой схемой [8], за счет сравнения результатов обработки в прямом и инвертированном представлении между собой.

Предлагаемое устройство шифрования данных в соответствии с алгоритмом Магма представлено на рис. 4. Устройство состоит из: внешнего интерфейса (например, шины данных), П — группы блоков шифрования данных в прямом представлении, И — группы блоков шифрования данных в инверсном представлении, блоков управления процессами шифрования, блока преобразования данных в/из инвертированного представления и сравнения результатов шифрования и блока синхронизации.

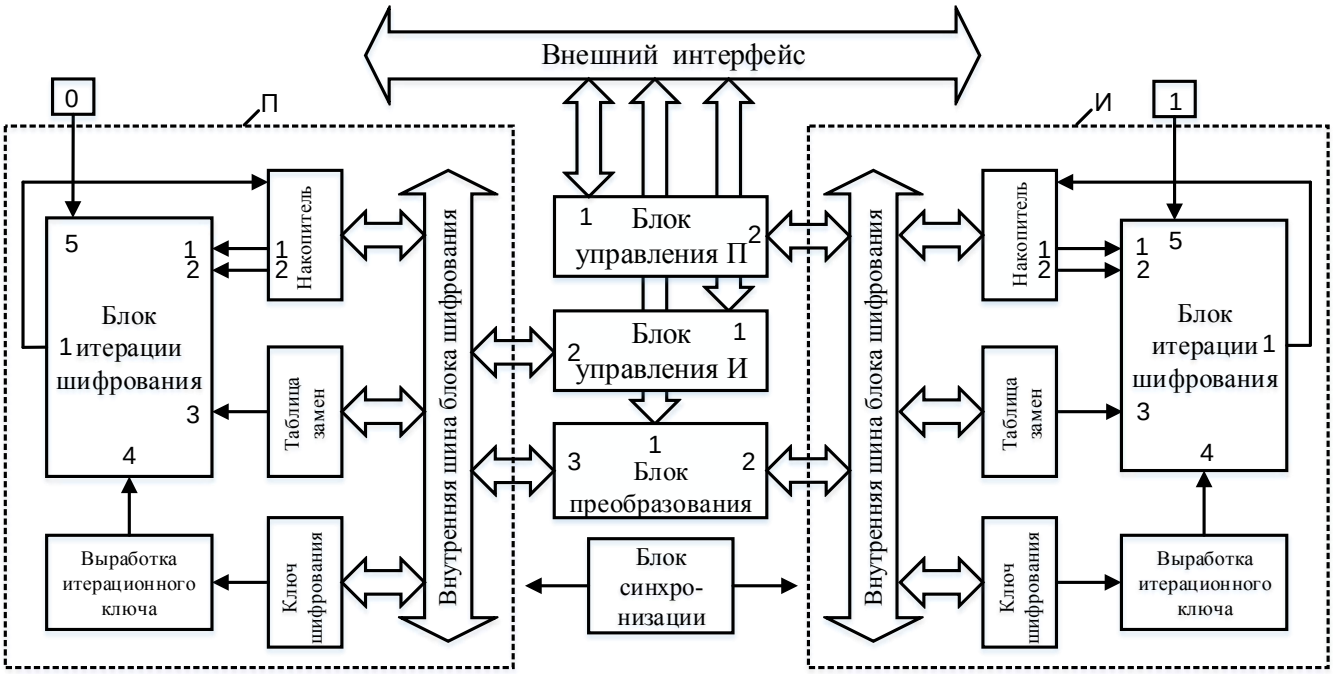


Рис. 4. Структура устройства шифрования

Блоки управления процессами шифрования и блок преобразования данных соединены с внешним интерфейсом. Второй вход/выход блока управления И соединен с внутренней шиной группы блоков И, а второй вход/выход блока управления П соединен с внутренней шиной группы блоков П.

Группы блоков П и блоков И идентичны друг другу и имеют следующий состав: внутренняя шина, блок накопитель шифруемых данных, блок хранения таблицы замен, блок хранения ключа шифрования, блок итерации шифрования данных, блок выработки итерационного ключа шифрования данных. Блок итерации шифрования данных имеет структуру, входы/выходы и функционирует в соответствии с приведенным ранее описанием.

Отличие группы блоков П и группы блоков И друг от друга заключается в том, что на пятый вход блока итерации шифрования в группе блоков П подают значение нуля, а в группе блоков И подают значение единицы. Эти значения определяют признак обработки в прямом и инвертированном представлении данных соответственно в группе блоков П и И.

Опишем работу устройства шифрования данных в соответствии с алгоритмом Магма.

Тактирование (синхронизация) всех блоков устройства осуществляется от единого тактирующего блока синхронизации.

До начала шифрования в устройство с внешнего интерфейса загружаются ключ криптографического преобразования и таблица замен. С внешнего интерфейса на блоки управления подают соответствующую команду, на вход блока преобразования данных подают ключ криптографического преобразования и таблицу замен. На основании поданной команды блоки управления формируют соответствующую команду или последовательность команд и подают их во внутренние шины блоков П и И. В блоке преобразования данных принятые ключ криптографического преобразования и таблица замен преобразуются в инвертированную форму, криптографический ключ и таблица замен в прямом и инвертированном представлении с третьего и второго выхода подаются в группу блоков П и И соответственно. В группах блоков П и И через внутренние интерфейсы ключи криптографического преобразования поступают в блоки хранения ключа шифрования, таблицы замен поступают в блоки хранения таблицы замен. Таблицы замен могут быть "жестко" прошиты в блоках хранения таблицы замен на этапах разработки или производства устройства.

С внешнего интерфейса на входы блоков управления подают соответствующую команду (зашифрование или расшифрование), на вход блока преобразования данных подают шифруемый блок или блоки данных. На основании поданной команды в блоках управления формируют соответствующие команды или последовательность команд и подают их во внутренние шины групп блоков П и И. В блоке преобразования данных шифруемые блоки данных преобразуют в инвертированную форму и в прямом представлении подают в группу блоков П, в инвертированном представлении подают в группу блоков И, в которых через внутренние шины шифруемый блок подают в блок накопителя шифруемых данных.

Далее осуществляют шифрование поданного блока данных в блоках П и И в соответствии с алгоритмом Магма, для этого на каждой итерации с блока накопителя на блок итерации шифрования подают шифруемые подблоки. Порядок подачи подблоков данных определяется в соответствии с выполняемой итерацией шифрования. Из блока таблицы замен в блок итерации шифрования подают таблицу замен, из блока хранения ключа шифрования в блок выработки итерационного ключа подают криптографический ключ. В блоке выработки итерационного ключа осуществляют выработку итерационного ключа в соответствии с текущей итерацией шифрования, и выработанный итерационный ключ подают в блок итерации шифрования. В блоке итерации шифрования осуществляют итерацию преобразования алгоритма Магма в соответствии с описанной выше процедурой. Результат шифрования из блока итерации шифрования подают в блок накопителя шифруемых данных. В блоке накопителя осуществляют сохранение зашифрованного подблока и обмен подблоков местами в соответствии с текущей итерацией шифрования. Аналогичным образом выпол-

няют все итерации в соответствии с алгоритмом Магма.

По завершению шифрования результат шифрования из блока накопителя через внутреннюю шину подают в блок преобразования данных. В блоке преобразования данных осуществляют сравнение результатов шифрования в блоках П и И. При соответствии результатов шифрования друг другу результат шифрования в прямом представлении с блока преобразования данных подается на внешний интерфейс. При несоответствии результатов шифрования друг другу блок преобразования данных формирует соответствующую команду или сигнал ошибки, который подают через внутренние шины на блоки управления.

Обсуждение предложенной структуры устройства шифрования

Предложенная авторами структура блока итерации шифрования и устройства шифрования в соответствии с алгоритмом Магма по стандарту ГОСТ Р 34.12-2015 не является единственно возможной. Как было уже отмечено, возможно применение различных оптимизационных схем, например, предложенных в [9, 11]. Предложенные в [9, 11] схемы оптимизации касаются в основном итерации шифрования и на них в полной мере распространяется особенность инверсной математики алгоритма Магма [1, 7], позволяющая введением внешнего признака переключать устройство итерации шифрования на работу с данными в прямом и инвертированном представлении. Необходимо отметить, что новизна предложенного решения заключается не в повышении достоверности вычислений, а в реализации защиты от утечек по каналам ПЭМИН при сохранении "классической" схемы повышения надёжности криптографических вычислений [8].

Эта особенность является замечательным свойством алгоритма Магма, позволяющим реализовывать обработку данных, представленных в прямом и инвертированном представлении на идентичных устройствах. Например, при реализации на устройствах по технологии FPGA для обработки данных в прямом и инвертированном представлении будет использоваться один и тот же код устройства. Особенно выигрышно это свойство будет проявляется при реализации устройств шифрования в виде интегральных схем.

При использовании оптимизации на уровне всего алгоритма шифрования Магма, таких как конвейеризация [8], распараллеливание обработки [12] и др., также сохраняют силу изложенные в исследовании предложения. В зависимости от конкретной схемы реализации алгоритма Магма, возможно возрастет число связей, требуемых для доставки признака обработки в прямом или инвертированном представлении данных до блоков сложения по модулю 2^{32}.

Изложенная особенность алгоритма Магма позволяет предположить, что разработка устройства шифрования, реализующего защиту от утечки информации по каналам ПЭМИН путем создания оптимальной маскирующей помехи за счет одновременной синхронной обработки данных в соответствии с алгоритмом Магма в прямом представлении и в инвертированном представлении и обеспечивающего повышение надежности криптографических вычислений за счет сравнения результатов обработки в прямом и инвертированном представлении между собой, возможна на уже созданных устройствах шифрования [8]. Возможно, подобная реализация не потребует или потребует минимальной аппаратной доработки устройств и в основном сведется к незначительному перепрограммированию FPGA устройств шифрования.

Одной из интересных задач дальнейшего исследования авторы видят в выяснении того, насколько универсальным является свойство изменения режима обработки данных между обработкой в прямом представлении и обработкой в инвертированном представлении за счет введения битового признака для наиболее распространённых алгоритмов шифрования.

Авторами были проведены экспериментальные исследования маскирования опасного сигнала с использованием равновесного кода [10]. Результаты, приведенные в [10], являются обнадеживающими, но при этом требуются

дополнительные экспериментальные исследования при реализации предложенного подхода в реальной аппаратуре.

Заключение

Приведенные в настоящем исследовании материалы представляют общую структуру устройств шифрования в соответствии с алгоритмом Магма по стандарту ГОСТ Р 34.12-2015. Разработанные структуры основаны на результатах предыдущих работ авторов, в части математического моделирования инверсных вычислений.

Предложенные структуры позволяют перейти к непосредственной разработке устройств шифрования, построенных на принципах защиты от утечки информации по каналам ПЭМИН путем создания оптимальной маскирующей помехи в соответствии с обоснованным в [6] подходом.

Работа подготовлена в рамках реализации программы ЛИЦ "Доверенные сенсорные системы" (Договор № 009/20 от 10.04.2020) при финансовой поддержке Минкомсвязи России и АО "РВК". Идентификатор соглашения о предоставлении субсидии — 0000000007119P190002.

Литература

1. *Амербаев В. М., Зверев Е. М., Куцепалов Н. О., Любушкина И. Е.* Собственная безопасность информационных криптошифраторов и методы ее реализации / Созидатели отечественной электроники. Вып. 5. Автор-составитель и редактор Малашевич Б. М. — М.: ТЕХНОСФЕРА, 2021. С. 410—448.

2. Сайт технического комитета по стандартизации ТК-26 [Электронный ресурс]. https://tc26.ru/ (дата обращения: 21.02.2022).

3. *Амербаев В. М., Шарамок А. В.* Защита ключевой информации от утечки по каналу ПЭМИН / Научно-практическая конференция "РусКрипто'2010", 1—4 апреля 2010 г.

4. *Шарамок А. В.* Аппаратная реализация ГОСТ 28147-89 для прозрачного шифрования потоков данных / Науч.-практ. конф. "РусКрипто'2013", 27—30 марта 2013 г.

5. ГОСТ 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры.

6. *Шарамок А. В.* Обеспечение структурной скрытности информативных сигналов побочных электромагнитных излучений и наводок // Специальная техника. 2011. № 3. С. 30—33.

7. *Lyubushkina I. E., Zverev E. M., Sharamok A. V.* Implementation of Information Security Devices in Equilibrium Codes// Journal of Theoretical and Applied Information Technology. 2020. V. 98. № 23. P. 3909—3920.

8. *Ракитин В. В.* Эволюция шифраторов семейства "Криптон". Фирма "АНКАД" — 25 лет на службе обеспечения информационной безопасности России / под ред. Романца Ю. В. — М.: ТЕХНОСФЕРА, 2016. С. 147—161.

9. Патент РФ № 2498416 C1, класс МПК H04L 9/06, G09C 1/00. Устройство шифрования данных по стандарту ГОСТ 28147-89: заявл. 15.05.2012 : опубл. 10.11.2013.

10. *Korotaev D. O., Slyusar V. V., Sharamok A. V., Bakhtin A. A.* Evaluation of the Effect of Desynchronization of Equilibrium Information Processing on the Effectiveness of Masking Information in Side-Channels // International J. Mechanical Engineering. 2021. V. 6(3). P.1736—1748.

11. *Винокуров А.* ГОСТ — не прост, а очень прост // Монитор. 1992. № 6–7. С. 14—19.

12. *Уэйкерли Дж. Ф.* Проектирование цифровых устройств. Т. 1. — М.: Постмаркет, 2002. — 544 с.

13. *Амербаев В. М., Шарамок А. В.* Криптографическое преобразование с двумерной сетевой структурой // Вопросы защиты информации. 2010. № 3. С. 12—16.

The structure of the Magma algorithm encryption device with a provision of calculations reliability and a protection against side channels leaking

[1] *A. A. Bakhtin*, [1] *E. A. Bordashevich*, [1] *E. M. Zverev*, [2] *I. E. Lyubushkina*, [1] *A. V. Sharamok*
[1] National Research University MIET, Zelenograd, Moscow, Russia
[2] "ANCUD" Ltd., Moscow, Russia

The article describes the structure of an encryption device implementing cryptographic data processing in accordance with the Magma algorithm with protection against information leakage through the side channels and increasing the reliability of cryptographic operations. Protection against information leakage by side channels is provided by creating an optimal masking interference. The optimal masking interference is created by simultaneous synchronous data processing in accordance with the "Magma" algorithm in the direct representation and in the inverted representation. The increase in the reliability of cryptographic operations is achieved due to the fact that in the encryption device, data is processed simultaneously in accordance with the Magma algorithm in direct representation and in inverted representation, followed by a comparison of the processing results in direct and inverse representation with each other. The proposed structure of the encryption iteration block allows the introduction of an external one-bit feature to switch the encryption iteration device to work with data in a direct or inverted representation.

Keywords: encryption device, encryption algorithm Magma, side channels, encryption, reliability.

Bibliography — 13 references. *Received September 2, 2022*

УДК 003.26
DOI: 10.52190/2073-2600_2022_3_13
EDN: VKCAOV

Альтернативный способ построения алгоритмов многомерной криптографии

Д. Н. Молдовян, канд. техн. наук
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН), Санкт-Петербург, Россия

Предложен новый способ реализации нелинейных отображений для построения новых алгоритмов открытого шифрования и электронной цифровой подписи, относящихся к многомерным криптосистемам — одной из областей постквантовой криптографии. Способ связан с заданием нелинейного отображения в виде операции возведения векторов с координатами в базовом поле GF(q) во вторую и третью степень как элементов конечной алгебры, являющейся расширением поля GF(q) степени $k \geq 2$. Применение отображений данного типа ориентировано на формирование открытого ключа в виде трудно обратимого нелинейного отображения с потайной лазейкой, представляющего собой суперпозицию двух нелинейных отображений и промежуточного линейного отображения перестановочного типа. Рассмотрены условия формирования конечных полей в форме конечных алгебр и вопросы выбора значений q и k. Разработанный способ предназначен для разработки новых алгоритмов многомерной криптографии, существенно сокращающих размер открытого ключа по сравнению с известными алгоритмами данного типа.

Ключевые слова: информационная безопасность, двухключевые криптосистемы, открытое шифрование, цифровая подпись, постквантовая криптография, многомерная криптография, конечная алгебра, конечное поле.

В связи с актуальностью разработки постквантовых стандартов на криптографические алгоритмы с открытым ключом [1] криптографическое сообщество уделяет значительное внимание проведению исследований в области многомерной криптографии [2—4]. Стойкость алгоритмов данного типа основана на вычислительной трудности задачи нахождения решения системы из многих степенных (обычно квадратных и кубичных в частных случаях [5]) с многими неизвестными, которая задана над конечным полем сравнительно малого порядка, равного, например, 16, 31, 256 [6] и 2^{16} [7]. Квантовый компьютер не является эффективным для решения таких систем, поэтому, если разработан алгоритм многомерной криптографии, обладающий требуемым уровнем стойкости к атакам с использованием обычных компьютеров, то он будет являться постквантовым. Однако алгоритмы многомерной криптографии обладают существенным для практического использования недостатком, состоящим в большом размере открытого ключа.

В настоящей статье предлагается новый способ построения алгоритмов многомерной криптографии со сравнительно малым размером открытого ключа.

Известные способы построения алгоритмов многомерной криптографии

Общая схема построения криптосхем многомерной криптографии состоит в задании способа формирования открытого ключа в виде набора из m многочленов второй или более высокой степени с коэффициентами и переменными, принимающими значения в поле $GF(q)$, которые описывают отображение $\mathcal{P}$

Молдовян Дмитрий Николаевич, научный сотрудник.
E-mail: mdn.spectr@mail.ru

Статья поступила в редакцию 30 июля 2022 г.

n-мерных векторов с координатами в поле $GF(q)$ в m-мерное векторное пространство над полем $GF(q)$. Для обеспечения возможности однозначного расшифровывания шифртекстов реализуется условие $m \geq n$. Значение m задает число уравнений, а n — число неизвестных в упомянутой ранее системе степенных уравнений. Открытый ключ описывает трудно обратимое нелинейное отображение с секретной лазейкой, с помощью которой его создатель может выполнить обратное отображение. При этом выполнение обратного отображения может включать операции, выходящие за рамки вычислений в поле $GF(q)$.

Для формирования открытого ключа выбирается некоторое нелинейное отображение $\mathcal{N}$, которое может быть представлено в виде набора полиномов над полем $GF(q)$ для которого можно с достаточной вычислительной эффективностью выполнит обратное отображение. Последнее служит потайной лазейкой, которая маскируется в открытом ключе путем формирования последнего в виде суперпозиции нелинейного отображения и одного или двух линейных $\mathcal{L}_1$ и $\mathcal{L}_2$ отображений, например, по формулам $\mathcal{P} = \mathcal{N} \bullet \mathcal{L}_1$, $\mathcal{P} = \mathcal{L}_2 \bullet \mathcal{N}$ или $\mathcal{P} = \mathcal{L}_2 \bullet \mathcal{N} \bullet \mathcal{L}_1$, где отображения $\mathcal{L}_1$ и $\mathcal{L}_2$ задаются в виде умножения отображаемого вектора на невырожденную матрицу размера $n \times n$ и $m \times m$ соответственно (данные матрицы задаются над полем $GF(q)$ и являются секретными).

Поскольку отображение $\mathcal{N}$ представимо в виде набора многочленов, описывающих координаты вектора-образа, переменными в которых являются координаты вектора-прообраза (отображаемого вектора), то легко записать отображение $\mathcal{P}$ в виде набора многочленов степени, равной степени многочленов, описывающих отображение $\mathcal{N}$. При этом за счет выполнения матричных умножений число слагаемых в многочленах, относящихся к $\mathcal{P}$, сильно увеличивается. Благодаря маскирующим линейным отображениям по набору из m многочленов, являющихся элементами открытого ключа, вычислительно трудно выполнить обратное отображение.

Открытое шифрование по ключу $\mathcal{P}$ выполняется следующим образом:

1. Шифруемое сообщение представляется в виде вектора $\mathbf{T} = (t_1, t_2, \ldots, t_n)$.

2. Шифртекст вычисляется в виде вектора $\mathbf{C} = \mathcal{P}(\mathbf{T}) = (c_1, c_2, \ldots, c_m)$.

Восстановление исходного сообщения из значения $\mathbf{C}$ выполняется как вычисление прообраза вектора $\mathbf{C}$:

$$\mathbf{T} = \mathcal{L}_1^{-1}(\mathcal{N}^{-1}(\mathcal{L}_2^{-1}(\mathbf{C}))) = \mathcal{L}_1^{-1} \bullet \mathcal{N}^{-1} \bullet \mathcal{L}_2^{-1}(\mathbf{C}).$$

Формирование электронной цифровой подписи (ЭЦП) к электронному сообщению D осуществляется владельцем открытого ключа $\mathcal{P}$ путем выполнения следующей процедуры (генерации ЭЦП):

1. Используя заранее согласованную хэш-функцию f_H, вычислить хэш-значение от сообщения D: $H = f_H(D)$.

2. Представить H в виде вектора $\mathbf{H} = (h_1, h_2, \ldots, h_n)$, координаты которого являются элементами поля $GF(q)$.

3. Вычислить подпись в виде прообраза вектора $\mathbf{H}$: $\mathbf{S} = \mathcal{L}_1^{-1} \bullet \mathcal{N}^{-1} \bullet \mathcal{L}_2^{-1}(\mathbf{C})$.

Проверка подлинности подписи $\mathbf{S}$ выполняется по открытому ключу $\mathcal{P}$ в соответствии со следующей процедурой (верификации ЭЦП):

1. Вычислить хэш-значение от сообщения D: $H = f_H(D)$.

2. Вычислить образ вектора $\mathbf{S}$: $\mathbf{H}' = \mathcal{P}(\mathbf{S})$.

3. Сравнить векторы $\mathbf{H}$ и $\mathbf{H}'$. Если $\mathbf{H} = \mathbf{H}'$, то подпись принимается как подлинная, в противном случае подпись отвергается.

Учитывая принцип построения двухключевых алгоритмов многомерной криптографии, достаточно понятно, что их существенным недостатком является большой размер открытого ключа. Для уменьшения размера открытого ключа, в частности, можно использовать отображения, описываемые прореженными многочленами (многочленами с малым числом слагаемых). В случае линейных отображений последнее достигается их заданием как умножение на прореженные невырожденные матрицы. Тем не менее, в известных алгоритмах рассматриваемого типа размер открытого ключа составляет от $1{,}6 \cdot 10^4$ [4] до $1{,}9 \cdot 10^6$ байт

[6] в зависимости от уровня обеспечиваемой стойкости и используемых отображений $\mathcal{L}_1$, $\mathcal{L}_2$ и $\mathcal{N}$.

Предлагаемый далее новый способ построения алгоритмов многомерной криптографии, обеспечивающий существенное уменьшение размера открытого ключа, состоит в формирование открытого ключа $\mathcal{P}$ в виде суперпозиции отображений, включающих два различных обратимых нелинейных отображения $\mathcal{N}_1$ и $\mathcal{N}_2$, например, по формулам $\mathcal{P} = \mathcal{N}_2 \bullet \mathcal{N}_1$ и $\mathcal{P} = \mathcal{N}_2 \bullet \mathcal{L} \bullet \mathcal{N}_1$, где линейное преобразование $\mathcal{L}$ задается в виде перестановки координат отображаемого вектора. Отображения $\mathcal{N}_1$ и $\mathcal{N}_2$ задаются в виде операций возведения во вторую или третью степень в конечном поле $GF(q^k)$, где $1 < k \le n$, представленном в форме конечной алгебры.

Задание конечных полей в виде конечных алгебр

Конечная m-мерная алгебра задается как m-мерное векторное пространство (над конечным полем), в котором дополнительно определена операция умножения всевозможных пар векторов, обладающая свойствами замкнутости и дистрибутивности слева и справа относительно операции сложения векторов. Произвольный вектор $A = (a_1, a_2, \ldots, a_m)$ можно представить в виде суммы его компонент $\mathbf{A} = \sum_{i=1}^{m} a_i \mathbf{e}_i$, где $\mathbf{e}_i$ — базисные векторы.

Операция умножения двух векторов $\mathbf{A}$ и $\mathbf{B} = \sum_{j=1}^{m} b_j \mathbf{e}_j$ определяется по правилу перемножения каждой компоненты первого вектора с каждой компонентой второго вектора, т. е. по формуле:

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

в которой каждое произведение вида $\mathbf{e}_i \mathbf{e}_j$ заменяется на однокомпонентный вектор $\lambda \mathbf{e}_k$, задаваемый таблицей умножения базисных векторов (ТУБВ). Значение λ называется структурной константой. Если $\lambda = 1$, то в таблице указывается базисный вектор $\mathbf{e}_k$. Левый множитель в произведении $\mathrm{e}_i \circ \mathrm{e}_j$ указывает строку, а правый — столбец, пересечение которых дает ячейку, содержащую значение $\lambda \mathbf{e}_k$. Свойства операции умножения и свойства алгебры определяются конкретным видом ТУБВ. Таблица 1 для произвольной размерности определяет коммутативную ассоциативную алгебру. Эта ТУБВ построена следующим образом. В первой строке расположены в упорядоченном виде все базисные векторы, а каждая следующая строка получена циклическим сдвигом предыдущей строки. Во всех ячейках расположенных ниже диагонали, проходящей из верхнего правого угла в нижний левый угол присутствует структурная константа λ. Если значение λ таково, что уравнение

$$x^m - \lambda = 0 \qquad (1)$$

не имеет решений, то m-мерная алгебра, заданная по табл. 1 над полем $GF(p^s)$, представляет собой конечное поле $GF((p^s)^m)$ [8, 9]. При условии делимости значения алгебра $p^s - 1$ на m существуют и легко находятся значения структурной константы λ, при которых (1) не имеет решения.

Тот факт, что табл. 1 задает конечное поле легко показать, учитывая, что в случае, когда уравнение (1) не имеет решений, многочлен $x^m - \lambda$ является неприводимым и множество всех многочленов степени $m - 1$ и менее с умножения многочленов по модулю $x^m - \lambda$ является полем $GF((p^s)^m)$. Между этим полем многочленов и алгеброй, заданной по табл. 1, имеется простой изоморфизм, состоящий в отображении многочленов вида $k_1 + k_2 x + k_3 x^2 + \ldots + k_m x^{m-1}$ в векторы вида $(k_1, k_2, k_3, \ldots k_m)$, который легко показать, рассматривая выполнение арифметического умножения произвольных двух многочленов и деление результата на неприводимый многочлен $x^m - \lambda$ и выполнение умножение соответствующих двух векторов по табл. 1. Указанный изоморфизм показывает, что рассматриваемая конечная алгебра является полем $GF((p^s)^m)$.

Таблица 1

Задание конечных полей вида $GF((p^s)^m)$ в виде конечных алгебр над полем $GF(p^s)$

·	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	…	…	$\mathbf{e}_m$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	…	…	$\mathbf{e}_m$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	…	…	$\mathbf{e}_m$	$\lambda\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	…	…	$\mathbf{e}_m$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	…	…	$\mathbf{e}_m$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_5$	…	…	$\mathbf{e}_m$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	…
…	…	…	$\mathbf{e}_m$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	λ…	…
…	…	…	λ…	λ…	λ…	λ…	…	$\lambda\mathbf{e}_{m-2}$
$\mathbf{e}_m$	$\mathbf{e}_m$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	:$\lambda\mathbf{e}_3$	:$\lambda\mathbf{e}_3$	…	$\lambda\mathbf{e}_{m-2}$	$\lambda\mathbf{e}_{m-1}$

Таким образом, имеется способ задания конечных расширений поля $GF(p^s)$ форме конечных алгебр, в которых операция возведения в квадрат (куб) может быть задана как вычисление значений набора из m многочленов второй (третьей) степени, заданных над полем $GF(q)$, где $q = p^s$. Как раз это и требуется для задания нелинейных отображений $\mathcal{N}_1$ и $\mathcal{N}_2$. Использование последних в алгоритмах многомерной криптографии предполагает их секретность. Секретным параметром может являться пара различных значений структурного коэффициента, использованных в первом и в втором нелинейных отображениях. Однако, желательно расширить пространство секретных параметров, что потенциально обеспечит более широкие возможности при разработке конкретных алгоритмов. Причем, такое расширение позволит выполнить каждое из нелинейных преобразований $\mathcal{N}_1$ и $\mathcal{N}_2$, осуществляя операции возведения в квадрат и в куб в полях $GF((p^s)^k)$ при $k < m$, например, при разных значениях k, являющихся делителями числа m. Последний прием позволяет существенно уменьшить размер открытого ключа.

Расширение пространства секретных параметров может быть достигнуто использованием нескольких структурных коэффициентов, имеющих различные распределения по ячейкам ТУБВ. Например, в табл. 1 могут быть введены еще $m - 2$ независимых структурных констант, которым могут быть назначены различные ненулевые значения. При этом каждая из этих структурных констант имеет уникальное распределение по ячейкам ТУБВ. Алгоритм генерации таких распределений приведен в [10]. Кроме того, при различных конкретных значениях m могут быть построены ТУБВ с различными распределениями базисных векторов, задающие поля в форме конечных алгебр $GF((p^s)^m)$. В последнем случае для каждого конкретного распределения базисных векторов имеется много различных распределений структурных констант, при которых реализуется алгебра в виде поля. Для размерностей $m = 5$, $m = 7$, $m = 11$ и др. такие примеры приведены в [11]. Случай задания полей в форме конечных алгебр по ТУБВ с нестандартным распределением базисных векторов представлены в табл. 2. и табл. 3.

Таблица 2

Задание конечных полей вида $GF((p^s)^5)$ в виде пятимерных конечных алгебр над полем $GF(p^s)$ с использованием четырех структурных констант τ, ε, μ и λ [11]

·	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\varepsilon\lambda\mathbf{e}_3$	$\tau\varepsilon\mathbf{e}_5$	$\tau\varepsilon\mu\lambda\mathbf{e}_1$	$\varepsilon\lambda\mathbf{e}_4$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\tau\varepsilon\mathbf{e}_5$	$\tau\varepsilon\mathbf{e}_4$	$\tau\mu\mathbf{e}_2$	$\tau\varepsilon\mu\lambda\mathbf{e}_1$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\tau\varepsilon\mu\lambda\mathbf{e}_1$	$\tau\mu\mathbf{e}_2$	$\mu\tau\mathbf{e}_5$	$\mu\lambda\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_5$	$\varepsilon\lambda\mathbf{e}_4$	$\tau\varepsilon\mu\lambda\mathbf{e}_1$	$\mu\lambda\mathbf{e}_3\mathbf{j}$	$\mu\lambda\mathbf{e}_2$

Таблица 3

Задание полей $GF((p^s)^7)$ в виде семимерных конечных алгебр при использовании ненулевых структурных констант δ, ρ, λ, ε, μ и τ [11]

·	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\rho\varepsilon\mu\mathbf{e}_4$	$\rho\varepsilon\mu\mathbf{e}_6$	$\rho\mu\tau\mathbf{e}_5$	$\delta\varepsilon\mu\mathbf{e}_7$	$\delta\rho\lambda\varepsilon\mu\tau\mathbf{e}_1$	$\rho\mu\tau\mathbf{e}_3$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\rho\varepsilon\mu\mathbf{e}_6$	$\rho\lambda\varepsilon\mathbf{e}_5$	$\delta\rho\lambda\varepsilon\mu\tau\mathbf{e}_1$	$\delta\lambda\varepsilon\mathbf{e}_2$	$\delta\lambda\varepsilon\mathbf{e}_7$	$\rho\lambda\varepsilon\mathbf{e}_4$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\rho\mu\tau\mathbf{e}_5$	$\delta\rho\lambda\varepsilon\mu\tau\mathbf{e}_1$	$\delta\mu\tau\mathbf{e}_7$	$\delta\mu\tau\mathbf{e}_3$	$\delta\lambda\tau\mathbf{e}_2$	$\rho\mu\tau\mathbf{e}_6$
$\mathbf{e}_5$	$\mathbf{e}_5$	$\rho\varepsilon\mu\mathbf{e}_7$	$\delta\lambda\varepsilon\mathbf{e}_2$	$\delta\mu\tau\mathbf{e}_3$	$\delta\varepsilon\mu\mathbf{e}_6$	$\delta\lambda\varepsilon\mathbf{e}_4$	$\delta\rho\lambda\varepsilon\mu\tau\mathbf{e}_1$
$\mathbf{e}_6$	$\mathbf{e}_6$	$\delta\rho\lambda\varepsilon\mu\tau\mathbf{e}_1$	$\delta\lambda\varepsilon\mathbf{e}_7$	$\delta\lambda\tau\mathbf{e}_2$	$\delta\lambda\varepsilon\mathbf{e}_4$	$\delta\lambda\tau\mathbf{e}_3$	$\rho\lambda\tau\mathbf{e}_5$
$\mathbf{e}_7$	$\mathbf{e}_7$	$\rho\mu\tau\mathbf{e}_3$	$\delta\lambda\varepsilon\mathbf{e}_4$	$\rho\mu\tau\mathbf{e}_6$	$\delta\rho\lambda\varepsilon\mu\tau\mathbf{e}_1$	$\rho\lambda\tau\mathbf{e}_5$	$\rho\lambda\tau\mathbf{e}_2$

Поле $GF((p^s)^m)$ в форме алгебры может быть задано при использовании в одной ТУБВ нескольких различных структурных констант с независимыми значениями, т. е. даже при сравнительно малых значениях порядка поля $GF(q)$ и размерности m пространство секретных параметров может быть достаточно большим.

Если операция возведения в квадрат (куб) в поле $GF((p^s)^m)$, заданном в виде конечной m-мерной алгебры, представлена в виде вычисления многочленов над полем $GF(p^s)$, то восстановление ТУБВ, по которой были получены эти многочлены не является тривиальной задачей, если в качестве секретного ключа использован набор значений нескольких структурных констант и конкретный вид распределения базисных векторов. При этом создатель набора указанных полиномов может легко выполнить обратную операцию (извлечение квадратного/кубичного корня), поскольку он знает конкретный вид поля $GF(p^s)$. Для этого он выполняет операцию возведения в целочисленную степень, равную значению 2^{-1} (3^{-1}) по модулю, равному порядку поля $GF((p^s)^m)$. Для реализации такой возможности требуется задать поле $GF((p^s)^m)$, порядок которого, а именно, значение $p^{sm} - 1$ не делится на два (три). Последнее замечание показывает, что при использовании полей $GF(p^s)$ нечетной характеристики нелинейное отображение следует задать как возведение в куб, а для полей четной характеристики — как возведение в квадрат. Возведение в степень больше трех представляют меньший интерес, поскольку их использование для задания нелинейных отображений приведет с существенному увеличению размера открытого ключа.

Варианты реализации нелинейных отображений

Рассмотрим задание нелинейных отображений $\mathcal{N}_1$ и $\mathcal{N}_2$ над полем $GF(2^8)$. Число $2^8 - 1 = 3 \cdot 5 \cdot 17$, поэтому определим $\mathcal{N}_1$ как возведение в квадрат векторов размерности $n = 3 \cdot 17 = 51$, а $\mathcal{N}_2$ — как возведение в квадрат векторов размерности $m = 5 \cdot 17 = 85$. Входным значением для операции отображения $\mathcal{N}_1$ предполагается 51-байтовое сообщение, представленное 51-мерным вектором, координатами которого являются отдельные байты сообщения (которые рассматриваются как элементы поля $GF(2^8)$). Входным значением для операции отображения $\mathcal{N}_2$ является 85-мерный вектор над полем $GF(2^8)$. Для согласования различных размерностей после операции $\mathcal{N}_1$ зададим выполнение линейного преобразования $\mathcal{L}$ в виде вставки 34 секретных байтов в выходной вектор операции $\mathcal{N}_1$, причем места вставки в общем случае предполагаются секретными.

Для реализации такой схемы построения двухключевого алгоритма многомерной криптографии для вычисления открытого ключа

требуется разработать две различные ТУБВ с несколькими структурными константами (для задания полей $GF((2^8)^{51})$ и $GF((2^8)^{85})$ в форме конечных алгебр). Для этого, ввиду достаточно большой размерности задаваемых алгебр, удобно использовать унифицированный вид ТУБВ, представленный в табл. 1. Использование унифицированного вида ТУБВ предполагает, что потенциальный атакующий знает распределение базисных векторов, используемых для задания отображений $\mathcal{N}_1$ и $\mathcal{N}_2$, однако он не знает распределения структурных констант и их значений. Для размерностей алгебр 51 и 85 могут быть найдены различные распределения для десятков структурных констант, каждая из которых может принимать одно из $\approx 2^8$ (знак приближенного равенства учитывает, что структурная константа не принимает нулевое и единичное значения) значений в поле $GF(2^8)$, т. е. имеется $\approx 2^{80}$ и более вариантов задания каждого из отображений $\mathcal{N}_1$ и $\mathcal{N}_2$. Это обосновывает предположение, что восстановление наборов структурных констант в ТУБВ, использованных для задания отображений $\mathcal{N}_1$ и $\mathcal{N}_2$, по коэффициентам в многочленах, описывающих открытый ключ, т. е. представление результирующего преобразования $\mathcal{P}=\mathcal{N}_2 \bullet \mathcal{L} \bullet \mathcal{N}_1$ в виде суперпозиции легко обратимых преобразований представляется вычислительно-трудной задачей.

Рассмотрим вопрос о размере открытого ключа в данной криптосхеме. Переменными в многочленах, составляющих открытый ключ, являются координаты входного вектора $\mathbf{X} = (x_1, x_2, \ldots, x_n)$. На выходе операции $\mathcal{N}_1$ получаем выходной вектор $\mathbf{Y} = (y_1, y_2, \ldots, y_n)$, каждая координата которого описывается квадратным многочленом второй степени, который включает 51 слагаемое в виде некоторого коэффициента k умноженного на произведение некоторых двух x-координат. Линейное отображение $\mathcal{L}$ не увеличивает размер многочленов, но увелчивает их число до 85. На входе операции $\mathcal{N}_2$ имеем вектор $\mathbf{U} = (u_1, u_2, \ldots, u_m)$, а на ее выходе — вектор $\mathbf{Z} = (z_1, z_2, \ldots, z_m)$, каждая координата которого описывается многочленом второй степени относительно переменных u_i ($i = 1, 2, \ldots, m$), который включает 85 слагаемых. Учитывая, что каждая переменная y_i' описывается многочленом, включающим 51 слагаемое вида kx_ix_j, устанавливаем, что z_i-координата описывается многочленом четвертой степени, включающим $85 \cdot 51^2$ слагаемых вида $k'x_ix_jx_kx_l$. Получаем общий размер набора всех коэффициентов, равный $85^2 \cdot 51^2 \approx 19$ Мбайт. При таком большом размере открытого ключа криптосхема становится непрактичной.

Заметим, что каждый отдельный многочлен в открытом ключе может быть представлен упорядоченным набором коэффициентов, расположенных, например, в порядке возрастания значения набора индексов (i, j, k, l) для случая несекретного распределения базисных векторов в ТУБВ. При использовании секретных ТУБВ потребуется открытый ключ расширить внесением в него упорядоченной последовательности наборов индексов входных переменных, которые задают соответствие коэффициента k' слагаемому $k'x_ix_jx_kx_l$ в каждом из многочленов открытого ключа. Далее рассмотрим построение криптосхем при использовании несекретного распределения базисных векторов, которое легко переносится и на случай использования секретных ТУБВ. В последнем случае размер открытого ключа несколько увеличивается.

Для построения алгоритмов с малым размером ключа каждое из нелинейных преобразований $\mathcal{N}_1$ и $\mathcal{N}_2$ следует задать как параллельное возведение в квадрат нескольких векторов. При этом размерность последних задается как делитель размерности n (в случае отображения $\mathcal{N}_1$) или m (в случае отображения $\mathcal{N}_2$), а влияние каждой координаты входного вектора на все координаты выходного вектора обеспечивается применением линейного преобразования $\mathcal{L}$ в виде достаточно простой перестановки координат векторов на выходе операции $\mathcal{N}_1$, которая формирует набор входных векторов операции $\mathcal{N}_2$, таких, что каждый из них включает по одной координате из каждого выходного вектора операции $\mathcal{N}_1$.

Рассмотрим конкретный пример $n = m = 35$. Входной вектор $\mathbf{X} = (x_1, x_2, \ldots, x_{35})$ операции

$\mathcal{N}_1$ представляем в виде каскада из 7 векторов: $\mathbf{X}=(\mathbf{X}_1,\mathbf{X}_2,\ldots,\mathbf{X}_7)$, где $\mathbf{X}_i=(x_1^{(i)},x_2^{(i)},\ldots,x_5^{(i)})$ для i = 1, 2,…, 7. Нелинейное отображение $\mathcal{N}_1$ реализуется как возводится в квадрат (например, с использованием табл. 2) каждого из векторов $\mathbf{X}_i$, формируя выходной вектор $\mathbf{Y}=(y_1,y_2,\ldots,y_{35})=(\mathbf{Y}_1,\mathbf{Y}_2,\ldots,\mathbf{Y}_7)$, где $\mathbf{Y}_i=$ $=(y_1^{(i)},y_2^{(i)},\ldots,y_5^{(i)})$ для i = 1, 2,…, 7. Линейное отображение зададим как перестановку координат векторов $\mathbf{Y}_1,\mathbf{Y}_2,\ldots,\mathbf{Y}_7$, описываемую следующей формулой:

$$u_i^{(j)}=y_j^{(i)},$$

где $u_i^{(j)}$ координаты каскада векторов $(\mathbf{U}_1,\mathbf{U}_2,\ \ldots,\mathbf{U}_5)=\mathbf{U}=(u_1,u_2,\ldots,u_m)$, причем $\mathbf{U}_j=(u_1^{(j)},u_2^{(j)},\ \ldots,u_5^{(j)})$ для j = 1, 2,…, 5. Нелинейное отображение $\mathcal{N}_2$ зададим как возведение в квадрат (например, с использованием табл. 3) каждого из векторов $\mathbf{U}_j$, что формирует выходной вектор $\mathbf{Z}=(z_1,z_2,\ldots,z_{35})=$ $=(\mathbf{Z}_1,\mathbf{Z}_2,\ldots,\mathbf{Z}_5)$, где $\mathbf{Z}_j=(z_1^{(j)},z_2^{(j)},\ldots,z_7^{(j)})$ для j = 1, 2,…, 5.

В такой криптосхеме открытый ключ представляет собой 35 многочленов, каждый член которых представляет собой коэффициент умноженный на произведение четырех переменных. Легко подсчитать, что число слагаемых в каждом многочлене равно $7\cdot5^2$, что дает размер открытого ключа, равный $35\cdot7\cdot5^2\approx$ 6 Кбайт.

В работе [12] приведена табл. 4, определяющая стойкость W алгоритмов многомерной криптографии к прямым атакам (атакам, основанным на нахождении решения системы степенных уравнений, полученной приравниванием многочленов открытого ключа к нулю) в зависимости от числа уравнений в случае равенства $n = m$. Рассмотренный последний пример задает построение алгоритмов со стойкостью к прямым атакам, равной 2^{100}. Для повышения стойкости можно взять аналогичное построение для случая $n = m = 85$ с использованием каскадов 5-мерных и 17-мерных векторов, заданных над полем $GF(2^8)$. Это дает 192-битную стойкость при размере открытого ключа, равном ≈36 Кбайт.

Таблица 4

Минимальное число уравнений (для случая $n = m$) над полем $GF(q)$, обеспечивающее заданный уровень стойкости к прямым атакам [12]

W	2^{80}	2^{100}	2^{128}	2^{192}	2^{256}
q = 16	30	39	51	80	110
q = 31	28	36	48	75	103
q = 256	26	33	43	68	93

В двух последних вариантах задания открытого ключа первое нелинейное отображение реализуется как возведение в квадрат векторов сравнительно малой размерности m_1 = 5. Смысл выполнения первой операции возведения в квадрат в алгебре меньшей размерности состоит в том, чтобы уменьшить размер открытого ключа, т. к. размер открытого ключа пропорционален третьей степени размерности m_1 и только второй степени размерности m_2. При выполнении этого правила для значений m_1 = 3–11 представляет интерес реализация первого нелинейного отображения с использованием операции возведения в третью степень. Это приводит к приемлемому увеличению открытого ключа (в m_1 раз) при ожидаемом существенном повышении стойкости к потенциальным структурным атакам (способам взлома криптосхемы без решения системы многих степенных уравнений с многими неизвестными [12]). Например, в последнем рассмотренном случае при использовании "кубичного" отображения $\mathcal{N}_1$ и "квадратичного" N_2 получаем открытый ключ в виде 85 многочленов шестой степени, имеющий размер ≈180 Кбайт, который при уровне стойкости 2^{192} значительно меньше по сравнению с этим параметром для известных алгоритмов многомерной криптографии.

Для получения достаточно малого размера открытого ключа второе нелинейное отображение следует задавать с использованием операции возведения в квадрат, выполняемой в поле $GF((q)^{m_2})$. Для того чтобы операция была однозначно обратима (т. е., чтобы суще-

ствовал единственный квадратный корень) в поле $GF((q)^{m_2})$ следует выбирать значения q, равные натуральным степеням числа 2. В этом случае $q^{m_2} - 1$ является нечетным значением и достигается требуемая однозначность обратного отображения. Если первое нелинейное отображение задается с использованием операции возведения в куб в поле $GF((q)^{m_1})$, то следует выбирать значения q, при которых число $q^{m_1} - 1$ не делится на число 3, что обеспечит однозначность извлечения кубического корня в поле $GF((q)^{m_1})$.

Одним из условий образования поля $GF((q)^k)$ в форме конечной алгебры является делимость числа $q - 1$ на k. С учетом этого легко видеть, что при равенстве размерностей входных и выходных векторов криптосхемы (т. е. при условии $m = n$) каждое из значений m_1 и m_2 должно нацело делить n и $q - 1$. При аналогичном построении криптосхем, в которых имеет место неравенство $m > n$, следует обеспечить выполнение делимости размерности входных векторов n на значение m_1 и делимости размерности выходных векторов m на значение m_2.

Заключение

Предложенный альтернативный способ построения двухключевых алгоритмов многомерной криптографии предоставляет потенциальную возможность повышения степени многочленов, составляющих открытый ключ, до 4 и 6 при обеспечении требуемого уровня стойкости и сравнительно малом размере открытого ключа. Предложенный способ базируется на использовании конечных полей, заданных в виде конечных алгебр, что определяет практический интерес к полям данного типа. Достигаемое увеличение степени многочленов представляет интерес как способ существенного повышения стойкости к структурным атакам, для чего ранее в работах [5, 13] предлагалось повышение степени до значения 3.

Вопросы разработки конкретных алгоритмов в соответствии с предложенным способом и рассмотрения структурных атак представляется самостоятельной задачей дальнейшего исследования.

Литература

1. Moody D. (2021) NIST Status Update on the 3rd Round, [online], https://csrc.nist.gov/CSRC/media/ Presentations/status-update-on-the-3rd-round/images-media/ session-1-moody-nist-round-3-update.pdf (дата обращения 11. 07.2022).
2. *Ding J., Petzoldt A.* Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. V. 15. № 4. P. 28—36.
3. *Kipnis A., Patarin J., Goubin L.* Unbalanced oil and vinegar signature schemes // EUROCRYPT 1999 procidings. Springer Lecture Notes in Computer Science. 1999. V. 1592. P. 206—222.
4. *Ding J., Schmidt D.* Rainbow, a new multivariable polynomial signature scheme // Conference on Applied Cryptography and Network Security — ACNS 2005. Springer Lecture Notes in Computer Science. 2005. V. 3531. P. 164—175.
5. *Sumit Debnath, Dheerendra Mishra*. Post-quantum digital signature scheme based on multivariate cubic problem // J. Information Security and Applications. 2020. V. 53. № 1.
DOI: 10.1016/j.jisa.2020.102512.
6. Rainbow Signature. One of three NIST Post-quantum Signature Finalists [on line] 2021. [Электронный ресурс]. Режим доступа: https://www.pqcrainbow.org/ (дата обращения: 11. 07.2022).
7. *Shuaiting Q., Wenbao H., Yifa L., and Luyao J.* Construction of Extended Multivariate Public Key Cryptosystems // International J. Network Security. 2016. V. 18. № 1. P. 60—67.
8. *Moldovyan N. A., Moldovyanu P. A.* Vector Form of the Finite Fields $GF(p^m)$ // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2009. № 3(61). P. 1—7.
9. *Молдовян Д. Н.* Расширение функциональности алгоритмов аутентификации и механизмы защиты информации над конечными группами векторов. Дисс. … канд. техн. наук. — СПб., 2012. — 138 с.
10. *Дернова Е. С.* Механизмы аутентификации информации, основанные на двух вычислительно трудных задачах. Дисс. … канд. техн. наук. — СПб., 2009. — 158 с.
11. *Молдовян Н. А.* Теоретический минимум и алгоритмы цифровой подписи. — СПб., БХВ-Петербург, 2010. — 304 с.
12. *Ding J., Petzoldt A.* Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. V. 15. № 4. P. 28—36.
13. *Baena J., Cabarcas D., Escudero D. E., Khathuria K., Verbel J. A.* Rank Analysis of Cubic Multivariate Cryptosystems // IACR Cryptol. ePrint Arch. 2018. DOI: 10.1007/978-3-319-79063-3_17.

Alternative method for developing algorithms of multivariate cryptography

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

A new method of implementing nonlinear mappings for constructing new algorithms for public encryption and electronic digital signature algorithms related to multivariate cryptosystems, that is one of the fields of post-quantum cryptography, is proposed. The method is associated with defining a nonlinear mapping in the form of an operation of raising vectors with coordinates in the base field GF(q) to the second and third degrees as elements of a finite algebra, which is an extension of the field GF(q) of degree $k \geq 2$. The use of mappings of this type is focused on the formation of a public key in the form of a one-way nonlinear mapping with a trap door, which is a superposition of two nonlinear mappings and an intermediate linear mapping of a permutation type. The conditions for the formation of finite fields in the form of finite algebras and the issues of choosing the values of q and k are considered. The developed method is intended for the development of new algorithms of multivariate cryptography, which significantly reduce the size of the public key compared to known algorithms of this type.

Keywords: information security, public-key cryptosystems, public encryption, digital signature, post-quantum cryptography, multivariate cryptography, finite algebra, finite field.

Bibliography — 13 references. *Received July 30, 2022*

УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004.056.52
DOI: 10.52190/2073-2600_2022_3_22
EDN: VLCXTF

Формирование модели управления правами доступа к информации

А. М. Трошков, канд. техн. наук; *М. А. Трошков*, канд. техн. наук;
А. Н. Ермакова, канд. эконом. наук; *С. В. Богданова*, канд. пед. наук;
А. В. Шуваев, д-р эконом. наук
ФГБОУ ВО «Ставропольский государственный аграрный университет», г. Ставрополь, Россия

Выявлены преимущественные процедуры процесса формирования модели управления правами доступа к информации в организациях. Проанализированы информационные потоки организации и подходы к техническому сопровождению моментов предоставления доступа персонала к информационному хранилищу, сведения о которых позволили предложить модель разграничения доступности корпоративной информации через ее сегментирование и мандатизацию пользователей. Особое внимание уделено детализации процессов определения мандатов на право доступа к информации и формирования грифов сегментов информационного поля. Результаты данного исследования можно использовать для разработки исполнительного инструментария предложенной модели, внедрение которой позволит повысить качество и оперативность исполнения управленческих решений по предоставлению прав доступа к информационному облаку организаций.

Ключевые слова: управление правами доступа, конфиденциальность, защита информационного облака, информационное поле, грифованность, мандат прав доступа.

Сегодня достаточно большое количество персонала организаций имеют разные права доступа к информационным ресурсам. Несмотря на то, что основным свойством информационных систем является разнообразие выполняемых задач, основными из них являются передача, прием и хранение данных. В связи с этим качество процессов циркуляции и хранения информации должно обеспечиваться через жесткую систему разрешений доступа к ней с учетом степени конфиденциальности предполагаемых к использованию данных. Целью исследования является акцентирование внимания на необходимости защиты информационных хранилищ организаций на основе разработки модели управления правами доступа к корпоративной информации.

Трошков Александр Михайлович, доцент, доцент кафедры "Информационные системы".
E-mail: troshkov1954@mail.ru
Трошков Михаил Александрович, доцент, научный сотрудник кафедры "Информационные системы".
E-mail: a-troshkov@mail.ru
Ермакова Анна Николаевна, доцент, доцент кафедры "Информационные системы".
E-mail: dannar@list.ru
Богданова Светлана Викторовна, доцент кафедры "Информационные системы".
E-mail: svetvika@mail.ru
Шуваев Александр Васильевич, профессор, профессор кафедры "Информационные системы".
E-mail: a-v-s-s@rambler.ru

Статья поступила в редакцию 22 августа 2022 г.

Методология

Основным методом исследования стал эмпирический метод. Наблюдение и эксперименты над изменением качества управления доступом к информационному хранилищу организации позволили систематизировать знания о подходах к организационному структурированию предприятия, вариантах сегментации его информационного поля, закрепления полномочий и мандатов пользователей информационной системы в рамках процедур

ограничения прав доступа к отдельным элементам информационного поля с целью формирования уникальной для данного предприятия системы доверительности и конфеденции.

Результаты

Выдвигая гипотезу о необходимости разработки алгоритма и механизма управления доступом к информационным ресурсам предприятия, проанализированы нормативно-правовые акты Российской Федерации, защищающие данные и устанавливающие ответственность, в том числе персональную, за разглашение или утечку защищенной информации. В процессе масштабирования использования информационных технологий человек все чаще сталкивается с проблемой защиты своих персональных данных и информации, с которой работает или предоставляет. Основу симбиоза человека и защищаемой информации составляет взаимодействие с техническими устройствами, что неизбежно приводит к необходимости её регламентации через инструментарий защиты информации. Для формирования эффективных операций обеспечения информационной безопасности недостаточно применять подходы, реализующие лишь методы и способы рационального хранения циркулирующей информации, еще необходимо формировать такие модели систем управления, которые в автоматическом режиме имеют возможность управлять права ми доступна персонала к отдельным сегментам и в целом информационному облаку.

Одним из действенных способов обеспечения защиты информационного облака по требованиям конфиденциальности, целостности и доступности является система управление правами доступа. Для проектирования её модели применен эмпирический метод исследования. Исходя из проведенного анализа научных работ в области информационной безопасности, сделан обобщающий вывод, что под сложным управлением правами доступа к информации понимается система алгоритмов, которая по определенным правилам разграничения доступности описывает процедуры разделения информационного хранилища на сегменты и мандатизации пользователей по ним. Проведенный глубокий анализ показал, что для моделирования системы управления правами доступа необходимо взять за основу:

- формальное представление системы разделения прав;
- бизнес-процесс дефрагментации доступности.

Наблюдения показали, что формальное представление требует существенных затрат и высокий коэффициент квалификации (K) специалистов, а бизнес-процесс имеет тенденцию вступать в противоречие между грифуемыми процессами. Исходя из этого, авторы предлагают использовать комбинированное направление моделирования системы управления правами доступа, преимущества которого представлены на рис. 1.

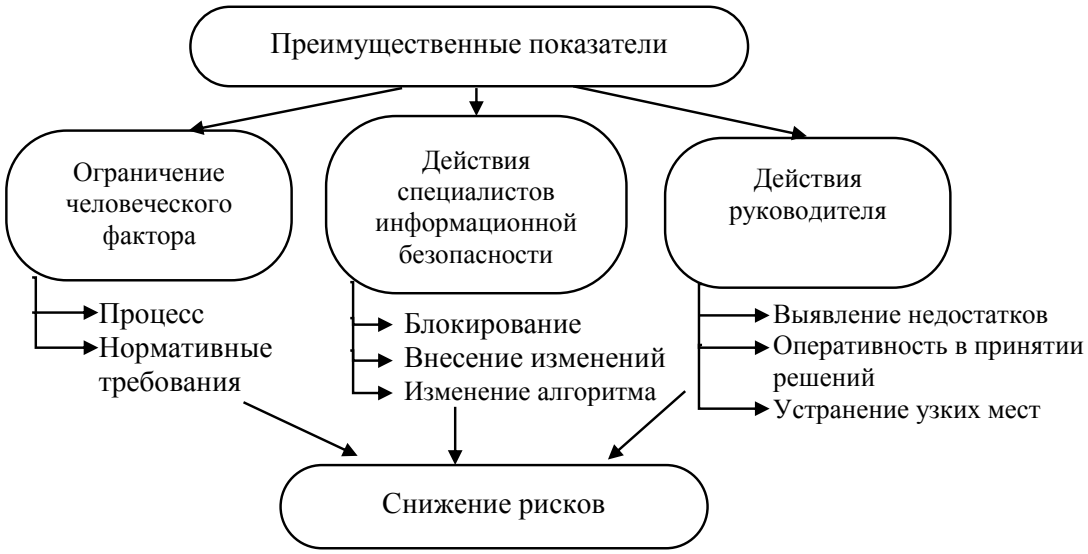


Рис. 1. Преимущества в управлении правами доступа

Рис. 2 иллюстрирует максимальную приемлемость в формировании модели системы управления правами доступа к информационному облаку организации предложенного комбинированно-направленного процесса со следующими этапами формирования исследуемой модели.

Из опубликованных материалов компании "IDS Scheer" были выявлены тенденции управленческих решений в России (рис. 3).

Анализ рис. 3 показал, что для формирования модели имеет смысл предложить основной способ обработки — графический, а для оформления результатов принятия решений в качестве дополнения использовать текстовую форму. Такие предложения закономерны, т. к. графическое описание удобно для формализации процессов проверки на корректность технических решений, кроме того, как было уже ранее доказано, восприятие образов более эффективно и позволяет оперативно изменять и вносить дополнения в модель.

Далее, из этапов формирования модели упорядочиваем алгоритмизацию процесса функционирования модели системы управления правами доступа к информации.

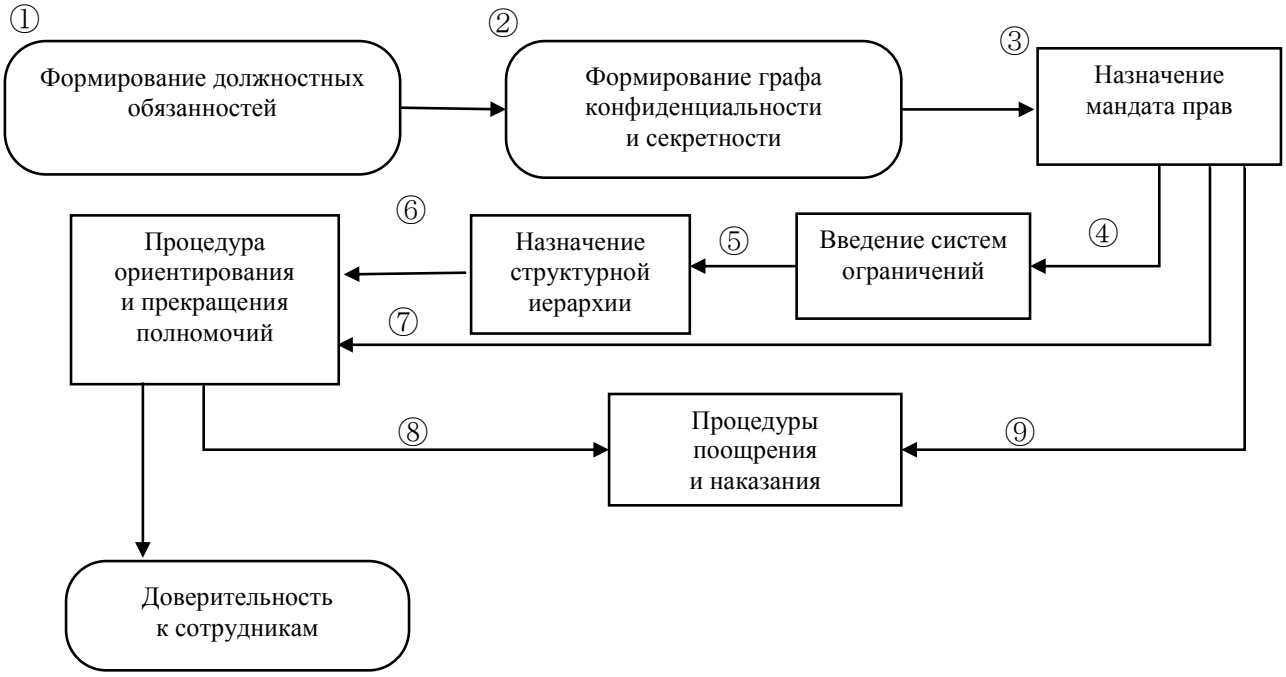


Рис. 2. Этапы формирование модели управления правами доступа к информации

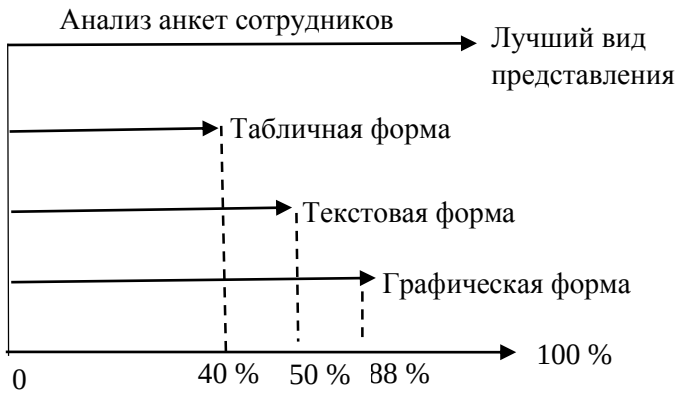


Рис. 3. Тенденции отображения для управленческих решений

На первом этапе руководство организации формирует должностные обязанности сотрудников в текстовой форме и определяет основной мандат на право доступа к информации (рис. 4).

На втором этапе необходимо сформировать грифы сегментов информационного поля (рис. 5).

В зависимости от должностных обязанностей персонала и степени грифованности документов предлагается назначить мандаты прав доступа в управлении циркулирующими информационными потоками и местами статического хранения информации (рис. 6).

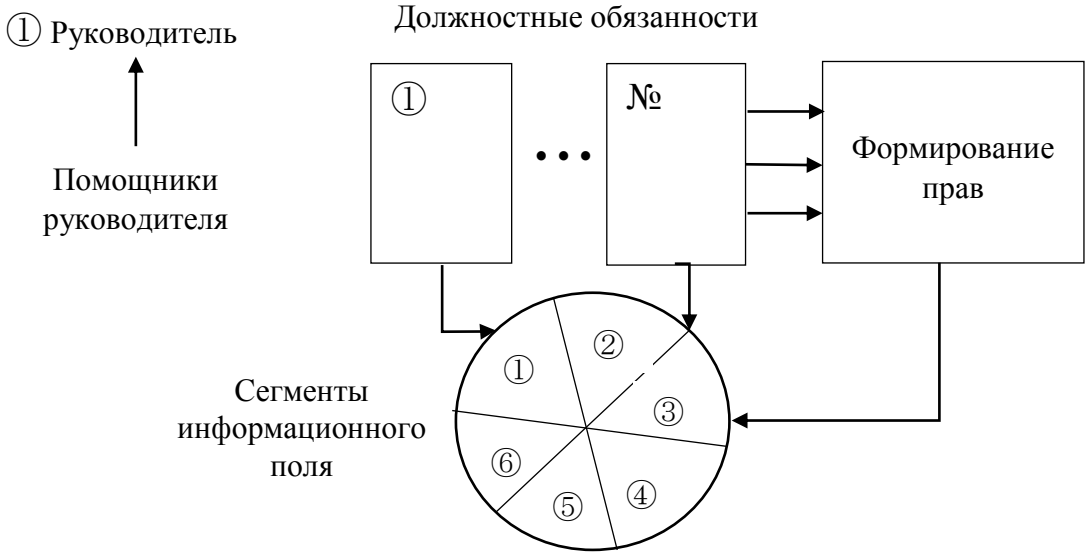


Рис. 4. Формирование должностных обязанностей и прав

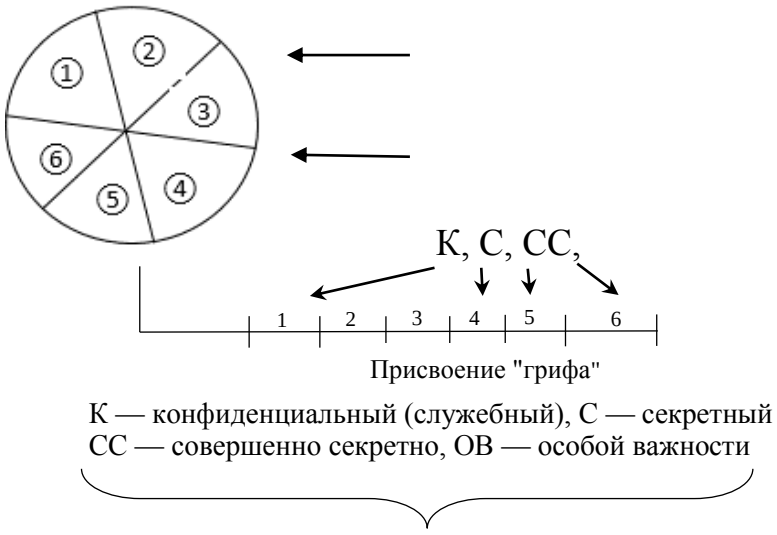


Рис. 5. Формирование степени грифованности сегментов информационного поля

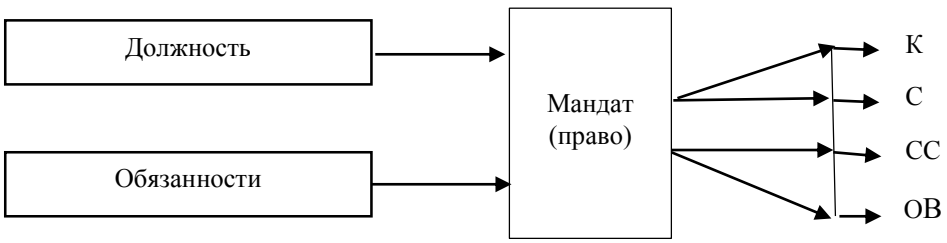


Рис. 6. Назначение мандатов прав доступа

В связи с тем, что проектируемая модель — "живая" структура с изменяющимися требованиями, обязанностями, иерархией подчинений, нарушениями, вводится система ограничений, представленная на рис. 7.

Архитектура предприятия, его организационно-штатная структура имеет определенную формацию, которая имеет тенденцию к изменению, как к увеличению, так и к уменьшению, а также плоскостное перемещение. Исходя из этого, предлагаем ввести понятие "Назначение структурной иерархии" (рис. 8).

С целью соблюдения эквилибра процедур в разрабатываемой модели вводим процедуру делегирования и прекращения полномочий (рис. 9), тем самым логически балансируя работу системы ограничений прав доступа (рис. 7), изменений структурной иерархии (рис. 8) и формирования должностных обязанностей.

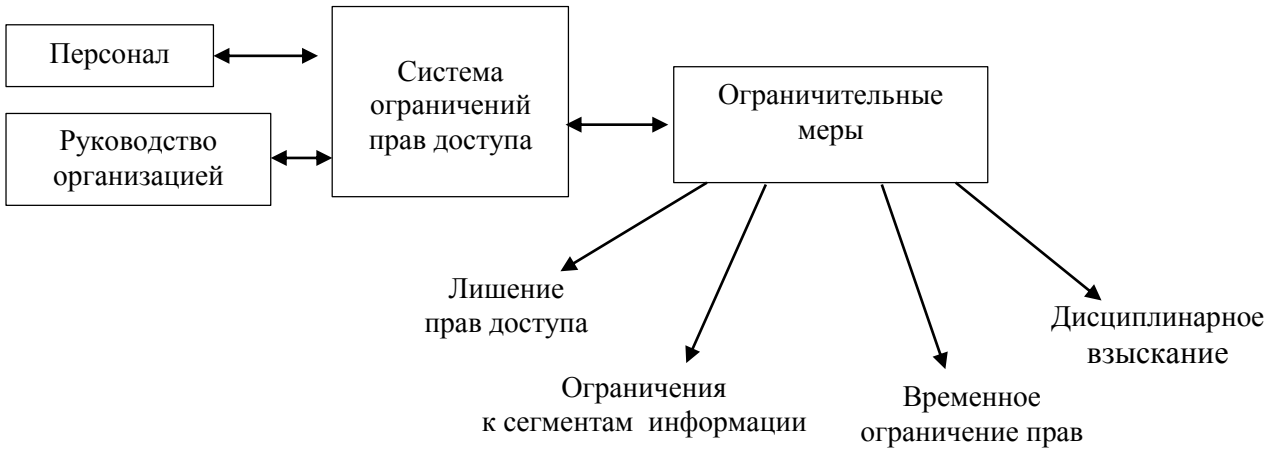


Рис. 7. Система ограничений прав доступа

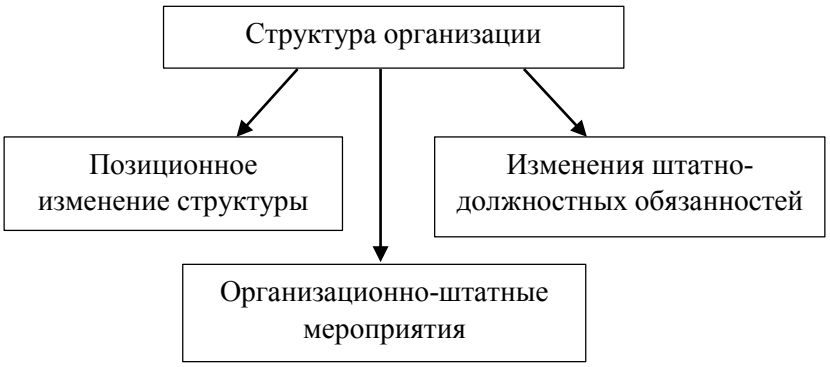


Рис. 8. Изменение структурной иерархии организации

Рис. 9. Процедура делегирования и прекращения полномочий

Исследования в системе управления правом доступа показали, что для качественной коллективной работы необходимо ввести процедуру "Доверительность", которая путем прохождения ряда этапов (рис. 10) позволит определить степень доверия к пользователям информационной системы и установит порог их конфеденции при доступе к различным данным.

Модель управления правами доступа к информации не будет целостной без процедуры поощрения и наказания за использование корпоративных информационных ресурсов (рис. 11).

Моделированные в исследовании процедуры призваны максимизировать эффективность функционирования системы управления правом доступа к информации.

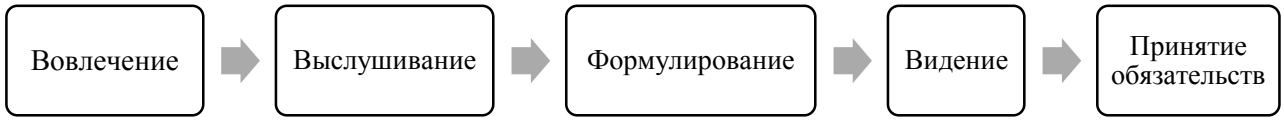


Рис. 10. Пять стадий формирования доверительных отношений

Рис. 11. Процедура поощрения и наказания в системе управления правом доступа к информации

Заключение

В целом инициируемые мероприятия по формированию модели системы управления правами доступа подтверждают целесообразность их применения в повседневной деятельности предприятий и организаций с целью обеспечения их информационной безопасности через описанный выше инструментарий информационной защиты.

Авторы благодарят экспертов ФГБОУ ВО "Ставропольский государственный аграрный университет", ФГАОУ ВО "Северо-Кавказский федеральный университет" и ООО "Компьютер-Союз" за советы и ценный вклад, как в проведение исследований, так и в коррекцию содержания статьи.

Литература

1. *Бородакий Ю. В., Добродеев А. Ю., Пальчун Б. П.* Система технических регламентов для критических объектов информатизации // Информационная безопасность. 2004. № 3.

2. *Громыко И. А.* Общая парадигма защиты информации // Защита информации. Инсайд. 2008. № 1. С. 12—18.

Formation of a mechanism for assigning trust and differentiating access rights to information resources of an enterprise

A. M. Troshkov, M. A. Troshkov, A. N. Ermakova, S. V. Bogdanova, A. V. Shuvaev
Stavropol State Agrarian University, Stavropol, Russia

The preferential procedures for the process of forming a model for managing information access rights in organizations are identified. The information flows of the organization, approaches to technical support of the moments of granting access to the information storage to the personnel are analyzed. They made it possible to propose a model for delimiting the availability of corporate information through its segmentation and user mandates. Particular attention is paid to detailing the processes of determining mandates for the right of access to information and the formation of labels for segments of the information field. The results of this study can be used to develop the executive tools of the proposed model. Its implementation will improve the quality and efficiency of execution of management decisions on granting access rights to the information cloud of organizations.

Keywords: access rights management, confidentiality, information cloud protection, information field, vulgarity, access rights mandate.

Bibliography — 2 references. *Received August 22, 2022*

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004
DOI: 10.52190/2073-2600_2022_3_29
EDN: VLKVFT

Актуальность и проблемы использования искусственных нейронных сетей в системах информационной безопасности

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

Сегмент информационной безопасности включает в себя ряд инновационных технологий, значительно повышающих эффективность работы информационных систем. Одной из наиболее актуальных и в то же время, имеющих ряд проблем технологий, являются искусственные нейронные сети. Основной целью представленной статьи является изучение вопроса актуальности и проблем интеграции искусственных нейронных сетей в сегменте информационной безопасности. В результате работы используются научные материалы зарубежного и отечественного авторства, а также применяются теоретические методы исследования. Научная значимость работы заключается в систематизации полученных знаний и возможности их использования в дальнейших исследованиях, касающихся тематики использования интеллектуальных технологий в сфере информационной безопасности.

Ключевые слова: искусственная нейронная сеть, обучение, информационная безопасность, информационная система, эффективность.

Распространение и становление информационных технологий является фактом в современном мире. Сегмент информационных технологий в течение последних десятилетий определял основные тенденции развития различных профессиональных секторов современного человека, основным из которых является технологический прогресс в целом. Развитие ИТ-рынка является основным направлением среди большинства развитых стран современного мира. Современный технологический прогресс отличается разработкой и становлением различных информационных технологий, способствующих повышению рациональности использования ресурсов и повышению эффективности работы современных предприятий. На сегодняшний день существует огромное множество прикладных и профессиональных задач, наиболее эффективное решение которых предполагает использования различного рода информационных технологий. ИТ-индустрия представляет из себя неотъемлемую часть профессиональной жизни современного человека [1].

Исходя из этого, особенную актуальность приобретают вопросы обеспечения информационной безопасности. Одной из наиболее значимых технологий для сферы защиты информации являются искусственные нейронные сети (ИНС). Именно посредством данного инструмента на сегодняшний день решаются одни из самых сложных и трудно-вычислимых задач. Далее в статье будут более подробно рассмотрены инструменты обеспечения информационной безопасности на основе ИНС, а также одни из наиболее эффективных и распространенных методов борьбы с переобучением в искусственных нейронных сетях.

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

Статья поступила в редакцию 11 июля 2022 г.

Методы

Автором используются теоретические и эмпирические методы исследования. В целях получения более подробной информации и актуальных данных в работе используются научные работы отечественного и зарубежного авторства. В результате работы автором используются научные материалы таких авторов, как: Цветкова О. Л., Крепер А. И., Бархатов Н. А., Ревунова Е. А., Ундалова И. С., Назаренко Ю. Л., Айдинян А. Р., Черняков П. В., Резник Д. В. и др. В каждой из данных работ затрагиваются фундаментальные вопросы, необходимые с целью воспроизведения общего анализа, касающегося использования искусственных нейронных сетей в аспекте информационной безопасности.

Таким образом, в используемой автором настоящей статьи литературе раскрываются такие вопросы, как: применение теории искусственных нейронных сетей в решении задач обеспечения информационной безопасности; возможности применения нейронных сетей в информационной инфраструктуре предприятия; использование нейросетей в рамках решения проблем кибербезопасности; анализ возможностей использования в целях обеспечения информационной безопасности и другие.

Основные риски информационной безопасности и используемые искусственные нейронные сети

Посредством ИНС может быть решен широкий круг задач из области защиты информации. Несмотря на такие возможности, некоторые из интеллектуальных инструментов для решения тех или иных задач находятся все еще на стадии разработки или же тестирования. Далее представлены основные риски информационной безопасности, решение которых может быть воспроизведено посредством ИНС [2]:

- нарушение данных — когда неавторизованный пользователь получает доступ к ценным и конфиденциальным данным, таким как информация о пользователе и кредитной карте;
- социальная инженерия — злоумышленники используют эту технику, чтобы манипулировать пользователями, чтобы предоставить им доступ или важные данные. Злоумышленники также могут комбинировать эту технику с другими кибератаками, чтобы, например, обманным путем заставить пользователей загружать вредоносное ПО;
- фишинг — это действие по отправке зараженных электронных писем или сообщений, замаскированных под законные, чтобы обманным путем заставить жертв предоставить личные и ценные данные или загрузить вредоносное ПО;
- внедрение структурированного языка запросов (SQL) — метод, используемый злоумышленниками для использования уязвимостей в серверах SQL для доступа к базе данных и запуска вредоносного кода. Идея SQL-i заключается в том, чтобы заставить сервер выполнять код и выполнять определенные действия, такие как раскрытие критической или иной секретной информации;
- атака типа "отказ в обслуживании" (DOS) — злоумышленники используют эту технику для наводнения сетей и серверов трафиком, вызывая утечку ресурсов и делая их недоступными;
- advanced Persistent Threats — атаки, способные обойти традиционные средства защиты и защиты периметра благодаря их скрытному характеру. APT используют механизмы сохранения, чтобы закрепиться в сети, собирая информацию о вашей ИТ-среде перед выполнением инициированной или рассчитанной по времени кибератаки [3].

При решении данных задач информационной безопасности используются различные виды нейронных сетей:

- нейронная сеть с прямой связью. Нейронная сеть с прямой связью — самая простая из всех разновидностей. Информация движется только в одном направлении и отправляется от входных узлов непосредственно к выходным узлам. В этой сети нет ни петель, ни циклов;
- рекуррентная нейронная сеть. В отличие от своего собрата с прямой связью, рекуррентная нейронная сеть позволяет передавать данные в двух направлениях. Этот тип сети

является популярным выбором для приложений распознавания образов, таких как решения для распознавания речи и рукописного ввода.

- модульная нейронная сеть. Модульная нейронная сеть состоит из независимых нейронных сетей. Каждому дается набор входных данных, и они работают вместе для выполнения подзадач. Конечный результат модульной нейронной сети управляется посредником, который собирает данные из отдельных сетей.
- сверточная нейронная сеть. Сверточные нейронные сети в основном используются для классификации изображений. Например, они могут группировать похожие фотографии и идентифицировать определенные объекты в кадре, включая лица, уличные знаки и людей.

Инструменты обеспечения информационной безопасности на основе искусственных нейронных сетей

Системы обнаружения и предотвращения вторжений (IDS/IPS). Эти системы обнаруживают вредоносную сетевую активность и предотвращают доступ злоумышленников к системам и предупреждают пользователя. Как правило, они распознаются по известным сигнатурам и общим формам атак. Это полезно против таких угроз, как утечка данных [4].

Глубокое обучение, сверточные нейронные сети и рекуррентные нейронные сети (RNN) могут применяться для создания более интеллектуальных систем идентификации/IP, анализируя трафик с большей точностью, уменьшая количество ложных предупреждений и помогая службам безопасности различать плохие и хорошие сетевые действия. Известные решения включают брандмауэр следующего поколения (NGFW), брандмауэр веб-приложений (WAF) и аналитику сущностей и поведения пользователей (UEBA).

Работа с вредоносным ПО. Традиционные вредоносные решения, такие как обычные брандмауэры, обнаруживают вредоносное ПО с помощью системы обнаружения на основе сигнатур. Компания ведет базу данных известных угроз, которая часто обновляет ее, чтобы включить новые угрозы, появившиеся недавно. Хотя этот метод эффективен против этих угроз, он с трудом справляется с более сложными угрозами.

Алгоритмы глубокого обучения способны обнаруживать более сложные угрозы и не зависят от запоминания известных сигнатур и распространенных шаблонов атак. Вместо этого они изучают систему и могут распознавать подозрительные действия, которые могут указывать на присутствие злоумышленников или вредоносных программ.

Обнаружение спама и социальной инженерии. Обработка естественного языка (NLP), метод глубокого обучения, может помочь вам легко обнаруживать и бороться со спамом и другими формами социальной инженерии. НЛП изучает нормальные формы общения и языковые модели и использует различные статистические модели для обнаружения и блокировки спама [5].

Анализ сетевого трафика. ИНС с глубоким обучением показывают многообещающие результаты при анализе сетевого трафика HTTPS для поиска вредоносных действий. Это очень полезно для борьбы со многими киберугрозами, такими как SQL-инъекции и DOS-атаки.

Аналитика поведения пользователей. Отслеживание и анализ действий и поведения пользователей — важная практика безопасности для любой организации. Это гораздо сложнее, чем распознать традиционные вредоносные действия против сетей, поскольку они обходят меры безопасности и часто не вызывают никаких флажков и предупреждений.

Основная проблема применения искусственных нейронных сетей в задачах информационной безопасности

Несмотря на все свои преимущества, эффективная разработка и использование ИНС затрудняется ввиду возникающих сложностей и задач, одной из которых является переобучения. На сегодняшний день активно используется целое множество методов борьбы с переобучением. Переобучение происходит в

случае, когда модель пытается предсказать тенденцию в слишком зашумленных данных. Это вызвано сложностью сети, имеющей слишком большое количество параметров. Переобученные ИНС являются неэффективны так как тренд не отражает реальность, представленную в данных. Данный факт подтверждается в том случае, если модель дает верные результаты на тренировочном наборе, но плохо работает на невидимых данных (тестовом наборе).

Основная цель обучения искусственной нейронной сети состоит в том, чтобы эффективно и правильно обобщать обучающие наборы на любые данные из предметной области. Это является важным фактором, так как основная задача состоит в том, чтобы в будущем модель смогла делать прогнозы на основе данных, которые она никогда раньше не "видела".

Первым шагом при работе с переобучением является уменьшение сложности модели. Чтобы уменьшить сложность, можно просто удалить слои или уменьшить количество нейронов. При этом важно рассчитать входные и выходные размеры различных слоев, задействованных в нейронной сети. Не существует общего правила относительно того, сколько нужно удалить или насколько большой должна быть ваша сеть. Но если нейронная сеть переобучается, первым делом необходимо попробовать ее уменьшить [6].

Методы борьбы с переобучением:

- ранняя остановка. Представляет метод регуляризации при обучении модели с помощью итеративного метода, похожего на градиентный спуск. Поскольку все нейронные сети обучаются исключительно с помощью градиентного спуска, ранняя остановка — это метод, применимый ко всем задачам;
- dropout. Основная идея, заложенная в данном методе, заключается в необходимости обучения не одного, а нескольких слоев искусственной нейронной сети с последующим усреднением результатов. Dropout представляет метод регуляризации, который приближается к параллельному обучению большого количества нейронных сетей с различной архитектурой.

Заключение

Таким образом, основной целью данной статьи являлось изучение вопроса актуальности и проблем интеграции искусственных нейронных сетей в сегменте информационной безопасности. В результате работы была изучена актуальность использования ИНС в задачах информационной безопасности, основные виды ИНС, используемых в данной отрасли, а также инструменты и проблемы их использования.

Как было выяснено, вовремя их обучения может возникнуть ряд проблем, затрудняющих точность и эффективность при работе систем информационной безопасности. Одной из таких проблем является переобучение, то есть явление, при котором построенная модель плохо работает на не участвовавших в обучении примерах. Для решения данной проблемы активно разрабатываются новые и уже давно используются на практике различные методы борьбы с переобучением.

Литература

1. *Цветкова О. Л., Крепер А. И.* О применении теории искусственных нейронных сетей в решении задач обеспечения информационной безопасности // Символ науки. 2017.
2. *Бархатов Н. А., Ревунова Е. А., Ундалова И. С.* Возможности применения нейронных сетей в информационной инфраструктуре предприятия // Инновационная экономика: перспективы развития и совершенствования. 2020.
3. *Ревунов С. Е., Бархатова О. М., Долгова Д. С.* Нейросетевые методы обеспечения информационной безопасности цифровой экономики // Инновационная экономика: перспективы развития и совершенствования. 2020. № 6(48). С. 79—84.
4. *Назаренко Ю. Л.* Использование нейросетей в рамках решения проблем кибербезопасности // European science. 2017. № 10 (32) С. 19—24.
5. *Резник Д. В.* Искусственные нейросети анализ возможностей использования в целях обеспечения информационной безопасности // The Scientific Heritage. 2021. № 67-1 (67). С. 50—53.
6. *Айдинян А. Р., Цветкова О. Л., Черняков П. В., Сокол Д. С.* Методики интеллектуального выбора и оценки DLP-системы для решения проблем информационной безопасности // Молодой исследователь дона. 2018. № 1 (10). С. 2—5.

Relevance and problems of using artificial neural networks in information security systems

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

The information security segment includes a number of innovative technologies that significantly increase the efficiency of information systems. Artificial neural networks are one of the most relevant and at the same time having a number of technology problems. The main purpose of the presented article is to study the relevance and problems of integration of artificial neural networks in the information security segment. As a result of the work, scientific materials of foreign and domestic authorship are used, as well as theoretical research methods are applied. The scientific significance of the work lies in the systematization of the acquired knowledge and the possibility of their use in further research related to the use of intelligent technologies in the field of information security.

Keywords: artificial neural network, training, information security, information system, efficiency.

Bibliography — 6 references. *Received July 11, 2022*

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2022.
Вып. 3 (138). С. 1—36.

Компьютерная верстка: *Н. В. Ильина, К. В. Трыкина*

Подписано в печать 26.09.2022. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 4,0. Уч.-изд. л. 4,2.
Тираж 400 экз. Заказ 2002. Свободная цена.
Адрес редакции: 125424, Москва,
Волоколамское ш., 77. ФГУП «НТЦ оборонного комплекса «Компас».
http://ntckompas.ru
Отпечатано: 101000, Москва,
Лубянский проезд, д. 15, стр. 4, офис 105.
ИП Кириченко Алексей Викторович.
Индекс 79187.

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

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

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

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

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

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

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

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

Комплектование статьи (обзора)

Статья должна быть представлена в редакцию в следующем комплекте:

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

Оформление статьи:

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

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

Оформление рисунков:

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

Оформление формул:

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

Оформление таблицы:

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

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

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

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