

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В СООТВЕТСТВИИ СО СХемой ВЗАИМОДЕЙСТВИЯ КОМПОНЕНТОВ

Коновалов К.А.

Московский Авиационный Институт, Москва, Россия

kkonov@gmail.com

Аннотация. В работе представлены средства защиты информации в соответствии со схемой взаимодействия компонентов для программной системы "Голосовая почта", на которых отработывалась модель динамической системы обеспечения комплексной защиты информации при перемещении информационных потоков. Наряду с предлагаемыми ранее средствами защиты при использовании данной системы предлагается механизм в виде дополнения подсистемой "Учета и контроля", а также механизмом "Мониторинга", включенных в общую схему защиты.

Ключевые слова: модель динамической системы, схема взаимодействия компонентов, защита информации, передача информации, система мониторинга, система учета и контроля, протокол взаимодействия.

Введение

Данная работа посвящена вопросам организации защиты информации в рамках специальной динамической модели при передаче голосовых сообщений по открытым каналам связи [1]. На данной модели отработываются возможные способы имитации взломов и их нейтрализация в узлах рассматриваемой системы. Предлагаемая распределенная система защиты реализуется на основе схемы взаимодействия компонентов программной системы "Голосовая почта", рассматриваемой в общем виде ранее [2], в указываемых критических точках возможного взлома.

Раскрывая содержание дополнительных средств необходимо еще раз повторить идею основных принципов, заложенных в систему защиты комплекса «Голосовая почта».

Основной принцип, закладываемый в схему – это распределение способов защиты для возможных точек взлома и локализация этих способов с учетом специфики рассматриваемой точки. Такое распределение учитывает целостность защиты и не позволяет по взлому одной точки защиты вскрыть общую схему функционирования защиты и обеспечить доступ к другим информационным ресурсам. Подобное распределение защитных средств включает не только общие механизмы, но и отдельные механизмы, которые применяются для каждого абонента и для сообщества абонентов голосовой почты. Это реализуется через модификацию передаваемых структур данных [3] и индивидуализацию программных подсистем [4]. Кроме этого было предложено множество наборов инструментов защиты, включая такие специфические возможности как водяной знак [5; 6], применяемых в комплексе.

Выше рассмотренные инструменты защиты так или иначе носят постоянный характер в рамках длительного промежутка времени. Предполагая случайность атак на систему и развитие методов её вскрытия, необходимо регулярно следить за подобными процессами. В связи с чем напрашивается подсистема постоянного мониторинга работы комплекса со службой системы учета и контроля [2]. Анализируя поведение атакующей стороны и моделируя способы их атак вырабатываются механизмы их нейтрализации. В этом случае после отработки механизмов нейтрализации не исключается вариант динамического изменения средств защиты. Кроме этого не исключается периодическое изменение защиты в тех или иных возможных точках взлома с учетом возможных временных рамок вскрытия такой защиты [1].

1. Три основных принципа построения системы и механизмы их обеспечения

В силу большого множества применяемых средств, требуется наглядность и понимание взаимодействия всех компонентов. Для этого была разработана схема работы программного комплекса «Голосовая почта», показанная на рисунке 1 в виде выделенных трех компонент, две из которых непосредственно участвуют в процессах приема-передачи, а третья компонента отвечает за вопросы учета и контроля. Последняя компонента выделена в обособленную ограниченную по доступу подсистему, с которой взаимодействие поддерживается не через открытые каналы связи (Интернет), а через специальные механизмы, исключающие удаленный доступ к данным. Ниже представлена концептуальная схема работы программного комплекса "Голосовая почта" (см. рисунок 1).

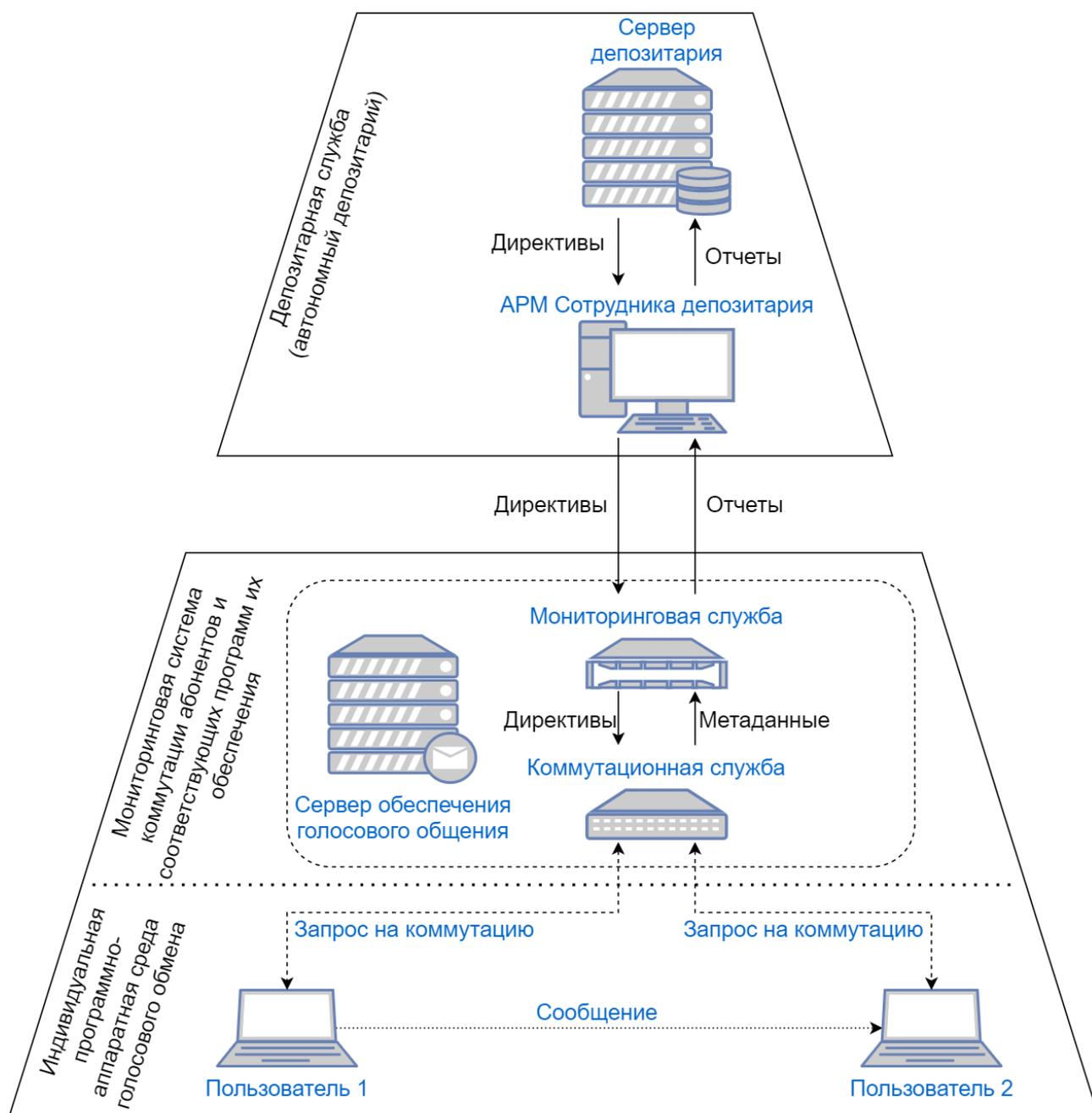


Рис. 1. Концептуальная схема работы программной системы "Голосовая почта"

Как указано на рисунке выше, передачу данных обеспечивают:

- **экземпляры программ пользователей** (названные индивидуальная программно-аппаратная среда голосового обмена) в основные задачи которых входит осуществление защищенного соединения для процесса приёма-передачи с другими аналогичными экземплярами программ пользователей, т. е. другими словами, это программы-абоненты;
- **мониторинговая система коммутации** (о необходимости данного компонента уже говорилось в предыдущих работах [1; 2; 3; 4; 5; 7; 8]), представляющая собой сервер, роль которого заключается в реализации механизма взаимодействия участников общения в виде экземпляров программ пользователей и недопущение подключения злоумышленника под видом легитимного пользователя;
- **депозитарная служба**, автономная часть, с которой поддерживается связь через посредника (внешний носитель, выделенная линия связи и пр.), на которую возложены задачи агрегирования и последующего хранения сведений участников общения для возможности учета и контроля выдаваемого программного обеспечения с проверкой со стороны мониторинговой системы коммутации.

В соответствии с требованиями по повышению качества и защищенности передачи, описанными в работе [1], предлагается реализовывать это за счет трех принципов:

- **Распределенность точек уязвимости** через снижение рисков по предполагаемым точкам уязвимости от успешно реализованных атак злоумышленников за счет переноса части функций с серверного компонента на клиентский, отказавшись от концентрации информации в одном месте. Данный подход предлагает в качестве реализации одного из требований осуществить перенос части функциональности с серверного компонента программной системы «Голосовая почта» на клиентский компонент, руководствуясь идеей старой английской поговорки «Don't put all your eggs in one basket» (Не клади все яйца в одну корзину). Перенос основывается на том факте, что серверный компонент рассматриваемой программной системы функционирует постоянно в режиме 24/7 и через него проходят все информационные потоки клиентов данной системы, формируемые самими клиентами, в то время как клиентский компонент функционирует небольшими интервалами времени без строго заданного расписания.
- **Динамичность смены политик** благодаря усилению контроля процесса приёма-передачи за счет дополнительных средств регулярной смены защиты, с учётом интервала времени вскрытия, зависящего от сложности предлагаемых механизмов защиты. В связи с требованиями по различным уровням защиты предлагается множество алгоритмов, включаемых в средства защиты и описываемых в соответствующих политиках.
- **Мониторинг процесса приёма-передачи**, поскольку, как уже говорилось ранее в работе [1], злоумышленник будет применять, для получения конфиденциальной информации, различные процедуры, направленные на анализ передаваемых потоков данных либо анализ кода программного продукта, предлагается учитывать при мониторинге процесса приема-передачи и при наличии предположений об атаке отрабатывать данную ситуацию на модели динамической системы обеспечения комплексной защиты.

2. Модель динамической системы

В рамках модели динамической системы предлагается механизм взаимодействия участников обмена информации таким образом [1], чтобы охватить задачи по реализации за счет механизмов использования различных вариантов кода программы и структур передаваемой информации, их периодического изменения, мониторинга процесса передачи, статистический сбор информации для учета и контроля всего процесса передачи. Для этих целей выделены и предлагаются следующие механизмы:

- Механизм **Маркирования** «водяными знаками» с целью дальнейшей идентификации (информация однозначно идентифицирует источник — экземпляр программного продукта).
- Механизм **Специальной структуризации** передаваемого потока данных (структуризация передаваемого потока амплитуд на базе качественного подхода к анализу данных для защиты от просмотра при перехвате).
- Механизм **Индивидуализации** (каждому пользователю создается персональный «индивидуальный» экземпляр программного продукта).
- Механизм **Распределения** разных типов обмена информации (каждый экземпляр соотносится с типом связи).
- Механизм **Учета и контроля**, где определяется объем необходимой информации о пользователе при обеспечении приёма-передачи (индивидуализация обеспечивает систему учета и контроля предоставления программного продукта).
- Механизм **Мониторинга**, обеспечивающий постоянный контроль за процессом приёма-передачи (на основе интегральной информации производится регулярный мониторинг использования программного кода и контроль процесса приема-передачи).
- Механизм **Статистики (Телеметрии)**, реализующий сбор информации необходимой для осуществления учета и контроля всего процесса взаимодействия участников процесса приёма-передачи.

Далее в работе освещается способ взаимодействия компонентов программной системы "Голосовая почта", определяемый механизмами «Учета и контроля» и «Мониторинга» при процессе приёма-передачи, т.е. экземпляров и мониторинговой системы коммутации, и описать схему их взаимодействия.

3. Формализация протокола взаимодействия компонентов

Теперь рассмотрим подробнее предлагаемую схему их взаимодействия, т. е. протокол взаимодействия. Основываясь на подходах, описанных в работах [9; 10; 11; 12], и целях в рамках данной работы, предлагается организовать взаимодействие, реализующее указанные на рисунке 1 запросы на коммутацию и передачу сообщений согласно рисунку 2, где П1 — Пользователь 1, П2 — Пользователь 2:

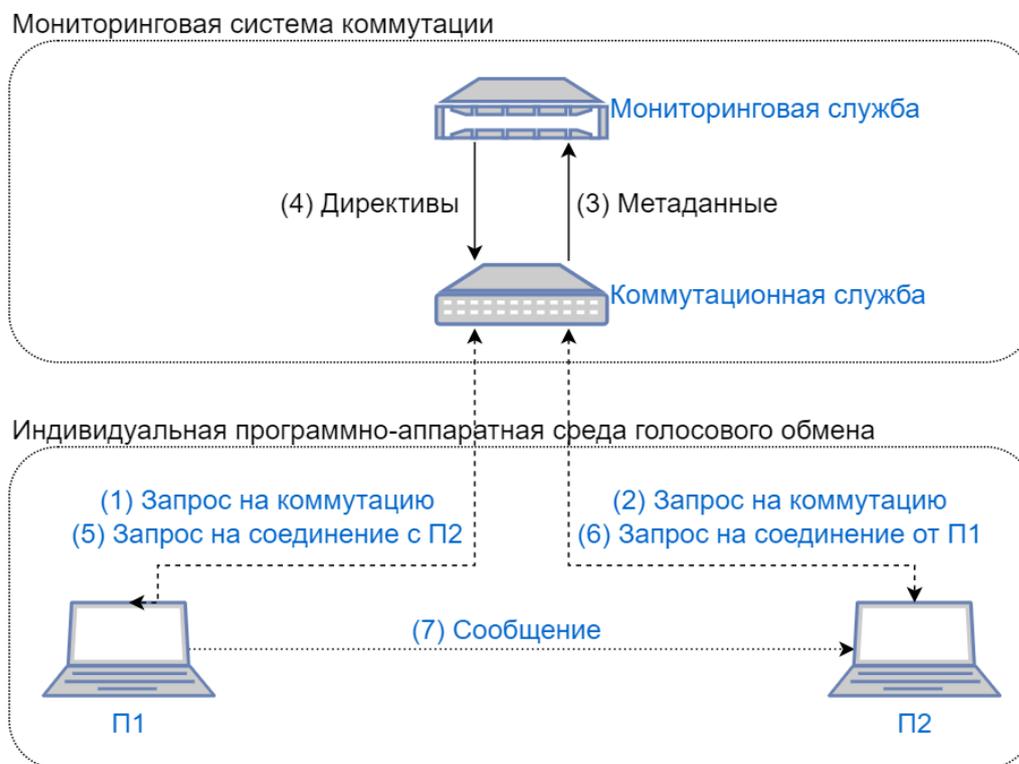


Рис. 2. Концептуальная схема работы программной системы "Голосовая почта"

Показанный на рисунке 2 принцип работы схемы взаимодействия для обеспечения работоспособности реализуется следующими обобщенными шагами:

- 1. производится запрос на коммутацию от П1, где коммутационная служба проверяет возможность взаимодействия;
- 2. производится перечень операций аналогичных пп. 1, но для П2;
- 3. информация пп. 1 и 2 в виде метаданных отправляется мониторинговой службе для проверки на нарушения;
- 4. при необходимости выполняются предписания;
- 5. П1 инициирует отправку сообщения П2, коммутационная служба проверяет его вхождение в среду общения П2;
- 6. П2 получает от коммутационной службы запрос на отправку от П1 сообщения;
- 7. при согласии П2 на получение сообщения от П1 производится загрузка.

Подробнее рассмотренные шаги следует разделить на ряд этапов. Обозначим шаг 1 и 2 из схемы выше подробнее этапами с 1 по 8, а шаги 5-7 этапами 9-11, пока, опустив шаги 3 и 4. На примере участников П1, П2 и «Коммутационная служба» подразумеваем, что П2 уже ранее прошел этапы с 1 по 8, поэтому он участвует с этапа 9:

- 1. П1, как инициатор взаимодействия, для процедуры приёма-передачи отправляет в мониторинговую систему коммутации (а именно коммутационной службе) служебное сообщение приветствия, указывая версию схемы взаимодействия и поддерживаемые экземпляром алгоритмы преобразования передаваемых данных. Кроме того, в приветственном сообщении содержится случайно сформированный набор байт, требующийся в последующих шагах данной схемы взаимодействия.
- 2. Коммутационная служба отвечает на сообщение приветствия экземпляра своим сообщением приветствия с указанием выбранного, из предложенного экземпляром списка, алгоритмом

преобразования передаваемых данных, добавив идентификатор взаимодействия и свой случайно сформированный набор байт. Кроме того, коммутационная служба отправляет данные для возможности экземпляром проверить достоверность коммутационной службы и запрашивает аналогичные сведения от экземпляра для обратной проверки.

- 3. П1 проверяет достоверность коммутационной службы по полученным данным на этапе 2.
- 4. П1 отправляет случайно сформированный набор байт из этапа 1 после выполнения над ним алгоритма преобразования передаваемых данных с параметром, полученным на этапе 2.
- 5. П1 отправляет случайно сформированный набор байт из этапа 1 после выполнения над ним алгоритма преобразования передаваемых данных с собственным параметром и данные для возможности коммутационной службой проверить достоверность экземпляра.
- 6. Коммутационная служба проверяет достоверность экземпляра по полученным данным из этапа 5.
- 7. П1 и коммутационная служба передают друг другу сообщение, объявляющее успешность процедур этапов 1-6, и меняют способ взаимодействия на обязательное применение выбранного алгоритма преобразования передаваемых данных: П1 отправляет коммутационной службе сообщение с применением алгоритма преобразования передаваемых данных, завершая подтверждение взаимодействия со своей стороны.
- 8. Коммутационная служба производит аналогичные действия по отношению к П1 из этапа 7.
- 9. П1 запрашивает взаимодействие с П1 у коммутационной службы.
- 10. Коммутационная служба отправляет экземплярам П1 и П2 данные по прямому взаимодействию между ними.
- 11. П1 и П2 начинают взаимодействие между собой напрямую, без участия коммутационной службы, реализуя обмен с использованием алгоритма преобразования передаваемых данных определенного на этапе 10.

Наглядно описанные выше действия представлены графически на рисунке 3.

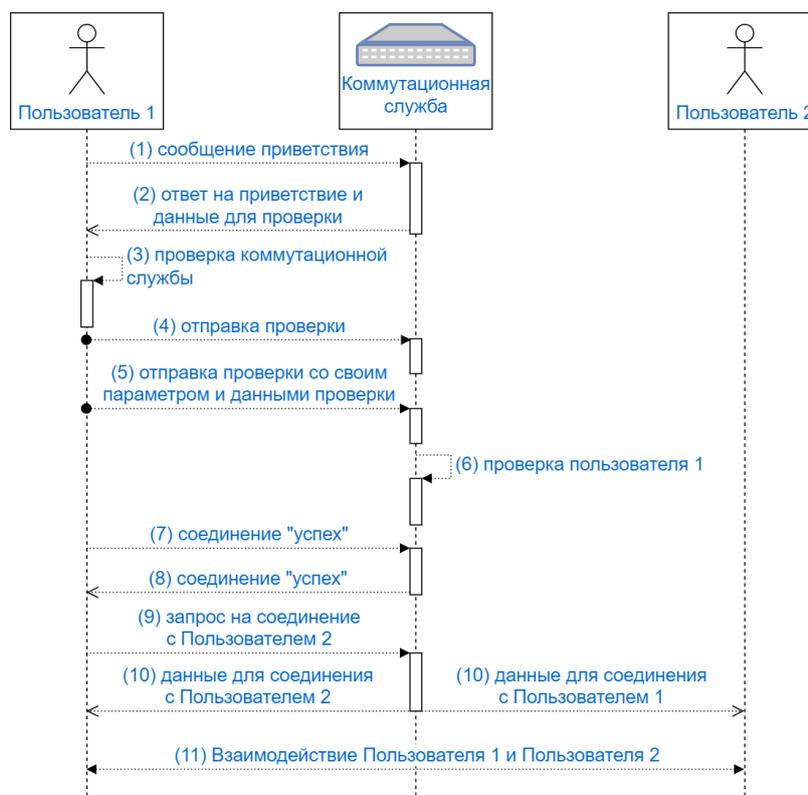


Рис. 3. Схема взаимодействия компонентов программной системы "Голосовая почта"

4. Заключение

Таким образом, была предложена схема работы и взаимодействия компонентов программной системы «Голосовая почта». Заложены ключевые принципы для достижения целей повышения

качества и защищенности передачи информации, реализуемые рассмотренными механизмами модели динамической системы обеспечения комплексной защиты информации.

Литература

1. Коновалов К.А., Балакирев Н.Е. Модель динамической системы обеспечения комплексной защиты информации при передаче голосовых сообщений. Информатика: проблемы, методы, технологии: сборник материалов XXII Международной научно-методической конференции - Воронеж, 2022 - С. 633-637
2. Коновалов К.А., Балакирев Н.Е. Создание системы обеспечения учета и контроля защиты информации при передаче голосовой информации. 20-я Международная конференция «Авиация и космонавтика». 22-26 ноября 2021 года. Москва. Тезисы. С. 231-233. ISBN 978-5-00189-750-7.
3. Думанский А.И., Федюк Ю.О., Балакирев Н.Е. Защита программного продукта через его индивидуализацию на примере модели голосовой почты. Гагаринские чтения - 2020. Сборник тезисов докладов. 2020. С. 294-295.
4. Селиванов Д.А., Думанский А.И., Балакирев Н.Е. Индивидуализация кода программ, учитываемых в депозитарии. XLVII Гагаринские чтения 2021. Сборник тезисов работ. 2021. С. 451-452.
5. Думанский А.И., Балакирев Н.Е., Зеленова М.В., Лазунин К.А., Фадеев М.М. Распределенная система защитных механизмов программного комплекса «Голосовая почта» на базе структуризации звукового потока волн. Информатика: проблемы, методы, технологии. Материалы XXI Международной научно-методической конференции. Воронеж, 2021. С. 709-716.
6. Фадеев, М.М. Возможные варианты алгоритмов нанесения водяные знаков для аудио информации / М.М. Фадеев, М.В. Зеленова, Н.Е. Балакирев // Информатика: проблемы, методы, технологии: Материалы XXI Международной научно-методической конференции, Воронеж, 11–12 февраля 2021 года. – Воронеж: Общество с ограниченной ответственностью "Вэлборн", 2021. – С. 922-929. – EDN FXNASP.
7. Думанский А.И., Семенова Т.Б., Бабуджи С.Ю., Балакирев Н.Е. Обеспечение конфиденциальной передачи информации через интернет. Гагаринские чтения — 2019. Сборник тезисов докладов. 2019. С. 337.
8. Федюк Ю.О., Балакирев Н.Е. Разработка различных стратегий использования голосовой почты с целью обеспечения дополнительных видов конфиденциальности. Гагаринские чтения - 2020. Сборник тезисов докладов. 2020. С. 523-524.
9. ГОСТ Р 34.10-2012 «Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
10. ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры».
11. Курганов Е.А. О глубине аппаратной реализации блочного шифра Кузнечик / Е.А. Курганов // Интеллектуальные системы. Теория и приложения. – 2016. – Т. 20. – № 1. – С. 61-78. – EDN XNAMCL.
12. Ищукова Е.А. Разработка и реализация высокоскоростного шифрования данных с использованием алгоритма Кузнечик / Е.А. Ищукова, Р.А. Кошущкий, Л.К. Бабенко // Auditorium. – 2015. – № 4(8). – С. 80-88. – EDN VARVPF.