УДК 004.056

Д. В. Бухаров, В. В. Кашковский

Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

ИССЛЕДОВАНИЕ УСТРОЙСТВА ШИФРОВАЛЬНОЙ МАШИНЫ «ЭНИГМА» И ВЫБОР ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ДЛЯ РАЗРАБОТКИ ЕЁ ЦИФРОВОЙ МОДЕЛИ

Аннотация. *В статье исследуются основные этапы развития криптографии с акцентом на шифровальную машину «Энигма», которая сыграла ключевую роль в обеспечении секретности коммуникаций в годы Второй мировой войны. Рассматриваются её конструктивные особенности, включая роторную систему, систему проводников и принцип работы механизма шифрования. Описывается алгоритм работы «Энигмы», который основан на сложной перестановке и подстановке символов, а также на изменении настроек машины для обеспечения динамической смены шифра. Важной частью работы является постановка задачи разработки цифровой модели «Энигмы», направленной на точное воссоздание её функциональности в современном контексте. Постулируются требования к модели, такие как точность симуляции работы механизма шифрования, а также возможность её применения в образовательных и научных целях. Особое внимание уделено выбору инструментальных средств для разработки цифровой модели, включая программные и аппаратные решения, такие как языки программирования, симуляторы и специализированные платформы, которые позволяют эффективно реализовать криптографические механизмы, заложенные в оригинальной машине. Автор анализирует подходы к моделированию, что предполагает как использование современных вычислительных ресурсов, так и учет исторических характеристик устройства. Статья будет полезна специалистам в области криптографии, компьютерной безопасности, а также исследователям в области истории криптографии и технической реконструкции. Результаты работы могут найти применение в учебных курсах по криптографии, а также в разработке инструментов для анализа и симуляции исторических криптографических систем.*

Ключевые слова: *цифровая модель, шифровальная машина, Энигма, разработка, инструментальные средства, шифрование, криптография.*

D. V. Bukharov, V. V. Kashkovsky

Irkutsk State Transport University, Irkutsk, Russian Federation

STUDY OF THE ENIGMA CIPHER MACHINE DEVICE AND SELECTION OF TOOLING FOR DEVELOPING ITS DIGITAL MODEL

Abstract. *The article investigates the main stages of cryptography development with a focus on the Enigma cipher machine, which played a key role in ensuring communication security during World War II. The paper discusses its design features, including the rotor system, wiring system, and the encryption mechanism's operation principle. The Enigma's algorithm, based on complex substitution and transposition of symbols, as well as changing the machine's settings to ensure dynamic cipher change, is described. An important part of the work is the formulation of the task of developing a digital model of the Enigma, aimed at accurately recreating its functionality in a modern context. Requirements for the model are outlined, such as the accuracy of simulating the encryption mechanism's operation and its potential application in educational and research settings. Special attention is given to the selection of tooling for developing the digital model, including software and hardware solutions such as programming languages, simulators, and specialized platforms, which allow for the efficient implementation of the cryptographic mechanisms embedded in the original machine. The author analyzes approaches to modeling, considering both the use of modern computational resources and the historical characteristics of the device. The article will be useful for specialists in the fields of cryptography, computer security, as well as researchers in the history of cryptography and technical reconstruction. The results may be applied in educational courses on cryptography and the development of tools for analyzing and simulating historical cryptographic systems.*

Keywords: *digital model, cipher machine, Enigma, development, tooling, encryption, cryptography.*

Введение

Целью данного исследования является исследование устройства шифровальной машины «Энигма» и выбор инструментальных средств для её разработки. Основная задача

заключается в анализе работы алгоритма шифрования, реализованного в этой машине, и выбор инструментальных средств, для её дальнейшей разработки.

Для достижения поставленной цели сформулированы следующие задачи:

1) Провести анализ принципов работы оригинальной шифровальной машины «Энигма»;

2) Выбрать программные средства, для разработки цифровой модели «Энигмы» с учетом всех особенностей ее конструкции и функционирования.

Объектом данного исследования является цифровая модель шифровальной машины «Энигма», разработанная на основе исторических данных и технических характеристик оригинала.

Актуальность исследования обусловлена необходимостью изучения классических методов шифрования и их применения в современных условиях. Несмотря на то, что «Энигма» была разработана в первой половине XX века, принципы её работы остаются интересными для исследователей криптографии и специалистов по информационной безопасности. Кроме того, изучение криптостойкости цифровых моделей исторических шифровальных машин может способствовать развитию новых подходов к созданию современных систем защиты информации.

Историческое развитие криптографии до появления «Энигмы»

Криптография как наука о защите информации имеет глубокие исторические корни, уходящие к древним цивилизациям. Еще задолго до создания первой механической шифровальной машины, такие личности, как Юлий Цезарь, использовали простые методы шифрования для защиты своих сообщений от перехвата [1].

Одним из первых известных методов шифрования является шифр Цезаря, который представляет собой простую замену каждой буквы алфавита другой буквой, сдвинутой на определенное количество позиций. Этот метод был прост в использовании, но легко поддавался криптоанализу при наличии достаточного количества зашифрованного текста.

С развитием письменности и дипломатических отношений между государствами потребность в более сложных системах шифрования стала очевидной. В Средние века начали появляться более сложные методы шифрования, такие как полиграммные шифры (например, шифр Виженера), которые использовали несколько различных ключей для шифрования одного сообщения [2, 3].

Рис. 1. Диск Альберти

В эпоху Возрождения и Нового времени криптографические методы продолжали совершенствоваться. Одним из значительных достижений того периода стал диск Альберти, изображённый на рисунке 1, созданный итальянским ученым Леоном Баттистой Альберти. Это устройство представляло собой два диска с нанесенными на них буквами алфавита, вращение которых позволяло осуществлять шифрование и расшифрование сообщений [4].

Однако настоящая революция в области криптографии произошла только в XX веке с появлением механических и электрических устройств для шифрования. Одним из таких устройств была шифровальная машина «Энигма», разработанная немецким инженером Артуром Шербиусом в начале 1920-х годов.

Создание и первые версии «Энигмы»

Шифровальная машина «Энигма» была разработана немецким инженером Артуром Шербиусом в начале 1920-х годов. Изначально она предназначалась для коммерческого использования, однако вскоре привлекла внимание военных и разведывательных служб Германии [5].

Первая версия «Энигмы» представляла собой электромеханическое устройство, состоящее из нескольких основных компонентов:

1) Роторная система: Набор роторов (вращающихся дисков с проводниками), каждый из которых имел свою уникальную конфигурацию соединений. При нажатии клавиши роторы поворачивались, меняя маршрут прохождения электрического сигнала через машину.

2) Ламповая панель: Отображала зашифрованную букву после каждого нажатия клавиши.

3) Клавиатура: Использовалась для ввода открытого текста.

4) Рефлектор: Специальный компонент, обеспечивающий симметричность шифрования (одна и та же настройка машины могла использоваться как для шифрования, так и для дешифрования).

Первоначально «Энигма» имела три ротора, которые могли быть установлены в разных позициях, что увеличивало сложность шифра. Однако уже в 1930 году были внесены изменения, включая добавление четвертого ротора и усложнение системы коммутации, что сделало машину еще более надежной [6-8].

Рис. 2. Шифровальная машина «Энигма»

Первые версии «Энигмы» использовались в основном для защиты коммерческой переписки и банковских транзакций. Однако вскоре немецкие военные увидели потенциал этого устройства и начали его массово использовать для шифрования стратегических сообщений [2, 7].

Алгоритм шифрования

Алгоритм шифрования, из используемый в машине «Энигма», основан на принципах полиалфавитного шифрования с использованием ротационных механизмов [3, 10]. Основные этапы процесса шифрования изображены на рисунке 3. и включают следующие шаги:

1) Инициализация настроек:

Перед началом шифрования оператор устанавливает начальную позицию роторов и выбирает порядок их расположения. Также может быть установлен дополнительный элемент — рефлектор, который определяет направление движения сигналов внутри машины.

2) Нажатие клавиши:

Когда оператор нажимает клавишу на клавиатуре, электрический сигнал проходит через систему, состоящую из роторов, рефлектора и коммутационной панели. Каждый ротор содержит набор контактов, соединенных таким образом, чтобы изменить путь сигнала при прохождении через него.

3) Поворот роторов:

После каждого нажатия клавиши первый ротор поворачивается на одну позицию. Когда этот ротор делает полный оборот, второй ротор поворачивается на одну позицию, и так далее. Это обеспечивает изменение маршрута сигнала при каждом новом символе, что делает шифр динамическим и сложным для анализа.

4) Прохождение через рефлектор:

После прохождения через все роторы сигнал попадает в рефлектор, который меняет направление его движения обратно через роторы. Это позволяет одной и той же настройке машины использоваться как для шифрования, так и для дешифрования.

5) Отображение результата:

На ламповой панели загорается лампа, соответствующая зашифрованному символу. Оператор записывает этот символ, и процесс повторяется для следующего символа исходного текста.

6) Расшифровка:

Для расшифрования используется тот же алгоритм, но в обратном порядке. Если настройки машины совпадают с теми, которые использовались при шифровании, то зашифрованный текст будет успешно преобразован обратно в открытый текст [4, 11, 14].

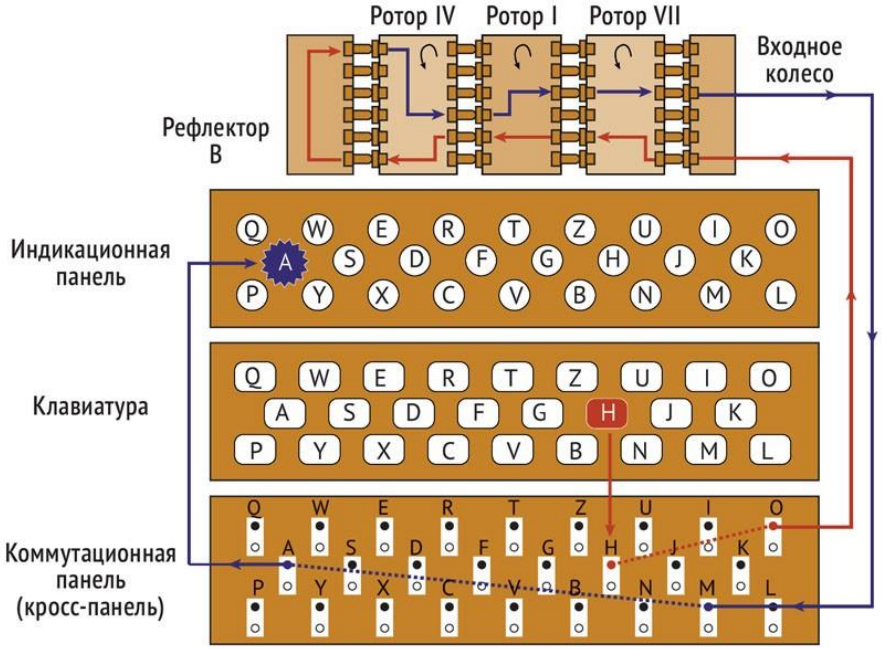

Рис. 3. Алгоритм шифрования

Цифровая модель шифровальной машины Энигма

Целью разработки цифровой модели шифровальной машины «Энигма» является создание программного обеспечения, которое будет точно воспроизводить работу оригинальной механической машины. Такая цифровая модель должна позволять проводить исследования криптографической стойкости алгоритмов шифрования, используемых в «Энигме», а также тестировать различные методы взлома и анализа шифротекстов.

Требования к цифровой модели:

1) Точность воспроизведения:

Модель должна максимально точно имитировать физические процессы, происходящие в оригинальной машине «Энигма».

Все компоненты (роторы, рефлекторы, коммутационные платы и т.д.) должны функционировать аналогично своим механическим прототипам.

2) Гибкость настройки:

Пользователь должен иметь возможность задавать начальные параметры машины (положение роторов, тип роторов, подключение штекеров и т.д.), соответствующие различным конфигурациям, использовавшимся во время Второй мировой войны.

Должна быть предусмотрена возможность изменения количества роторов и их типа.

3) Удобство использования:

Интерфейс программы должен быть интуитивно понятным и удобным для пользователя.

Программа должна предоставлять возможности для ввода и вывода данных в различных форматах (текстовые файлы, консольный ввод-вывод и т.д.).

4) Производительность:

Скорость выполнения операций шифрования и дешифрации должна быть достаточно высокой для проведения масштабных экспериментов.

5) Модульность:

Код программы должен быть структурирован таким образом, чтобы отдельные модули можно было легко заменять или модернизировать.

6) Документирование:

Подробная документация по использованию программы, включая описание всех параметров и настроек.

7) Тестирование:

Проведение тестирования цифровой модели на соответствие оригинальным спецификациям «Энигмы».

Выбор средств разработки

При разработке цифровой модели шифровальной машины «Энигма» необходимо учитывать ряд факторов, таких как точность моделирования, производительность, удобство использования и совместимость с различными операционными системами.

Исходя из этих требований, выбор средств разработки включает следующие аспекты:

1) Язык программирования: Для реализации цифровой модели могут использоваться различные языки программирования, такие как Python, C++, Java и другие. Python является популярным выбором благодаря своей простоте, читаемости кода и наличию обширной библиотеки для научных расчетов и симуляции. C++ обеспечивает высокую производительность и контроль над ресурсами системы, что важно для сложных вычислительных задач. Java предоставляет хорошую кросс-платформенную поддержку и развитые инструменты для разработки графического интерфейса пользователя (GUI).

2) Библиотеки и фреймворки: Использование специализированных библиотек и фреймворков поможет ускорить разработку и повысить качество конечного продукта. Например, библиотека NumPy в Python может быть использована для работы с массивами данных и математических операций, а библиотека PyQt или Tkinter — для создания GUI. В случае выбора C++, можно использовать библиотеки вроде Boost для повышения производительности и удобства разработки.

3) Инструменты для моделирования и симуляции: Существуют специализированные программные пакеты для моделирования физических систем, например, Simulink от MathWorks. Однако для более узкоспециализированных задач, связанных с шифрованием, возможно потребуется разработать собственные модули или использовать существующие библиотеки, ориентированные на криптографию.

4) Среда разработки (IDE): Выбор интегрированной среды разработки (IDE) зависит от предпочтений разработчика и используемого языка программирования. Популярные IDE включают Visual Studio Code, PyCharm, Eclipse и другие. Эти среды предоставляют удобные функции для редактирования кода, отладки и управления проектами.

5) Система контроля версий: Важно использовать систему контроля версий, такую как Git, для отслеживания изменений в коде и совместной работы над проектом. Это особенно полезно при работе в команде и для документирования истории изменений.

6) Тестирование и верификация: Необходимо предусмотреть средства для тестирования и верификации цифровой модели. Это может включать автоматическое тестирование отдельных модулей и интеграционное тестирование всей системы. Также следует провести сравнительный анализ результатов шифрования с известными историческими данными для проверки точности модели.

7) Документация и комментарии: Создание подробной документации и комментариев к коду облегчит понимание проекта другими исследователями и упростит дальнейшую модификацию и расширение модели.

Исходя из вышеперечисленных аспектов выбраны следующие средства разработки:

1) Python идеально подходит для создания цифровой модели шифровальной машины «Энигма», потому что он позволяет быстро разрабатывать сложные алгоритмы шифрования и моделировать поведение механических компонентов машины. Его простота и гибкость делают его отличным инструментом для исследовательских проектов, где важна скорость разработки и возможность быстрой адаптации кода под новые требования.

2) Библиотеки и фреймворки: QT Designer необходим для создания удобного и привлекательного графического интерфейса для цифровой модели «Энигмы». Это позволит пользователям легко настраивать параметры машины, вводить данные и получать результаты шифрования. Кросс-платформенность QT Designer гарантирует, что программа будет доступна широкому кругу исследователей независимо от их операционной системы.

3) Среда разработки (IDE): Sublime Text является мощным текстовым редактором, который отлично подходит для работы с кодом на Python. Он предлагает удобный интерфейс, высокую скорость работы и возможность настройки под индивидуальные потребности разработчика. Это идеальный инструмент для написания и отладки кода цифровой модели «Энигмы».

4) Система контроля версий: Git необходим для управления версионностью кода и координации работы команды разработчиков. Это особенно важно в исследовательском проекте, таком как исследование криптографической стойкости цифровой модели «Энигмы», где требуется тщательный учет всех изменений и возможность возврата к предыдущим версиям кода.

Разработка архитектуры цифровой модели

Архитектура цифровой модели шифровальной машины «Энигма» играет ключевую роль в обеспечении точности и эффективности ее функционирования.

Основная цель разработки архитектуры заключается в создании структуры, которая будет максимально приближена к оригиналу, сохраняя при этом возможность адаптации к современным вычислительным ресурсам и требованиям.

Основные элементы архитектуры:

1) Моделирование роторов: Каждый ротор представлен отдельным объектом, содержащим информацию о его конфигурации (подключение контактов, шаг поворота и т.д.). Роторы взаимодействуют друг с другом согласно правилам механики оригинальной машины.

2) Коммутационная плата: Моделирует физическое соединение роторов и других компонентов машины. Реализует передачу сигналов между роторами и контролирует их поворот после каждого шага шифрования.

3) Рефлектор: Представлен как отдельный модуль, отвечающий за отражение сигнала назад через роторы. Конфигурация рефлектора задается в соответствии с выбранной моделью «Энигмы».

4) Интерфейс пользователя: Включает в себя графический интерфейс для ввода и вывода данных, а также настройки параметров машины (начальная позиция роторов, подключение штепселей и т.д.). Этот элемент архитектуры обеспечивает удобство использования модели и позволяет проводить эксперименты в интерактивном режиме.

5) Алгоритмическая логика: Определяет последовательность шагов шифрования и дешифрования, а также правила взаимодействия между компонентами машины. Логика должна строго следовать оригинальному процессу работы «Энигмы».

6) Система хранения данных: Предусматривает хранение текущих состояний машины, а также результатов проведенных экспериментов. Это позволяет анализировать полученные данные и сравнивать их с исторически известными примерами.

Заключение

В ходе исследования было продемонстрировано, как устройство и алгоритм работы шифровальной машины «Энигма» могут быть воссозданы в цифровой форме с использованием современных инструментальных средств. Разработка цифровой модели шифровальной машины позволит глубже понять принципы её функционирования и провести анализ уязвимостей в контексте исторического применения. Этот подход может быть полезен для образования и исследования криптографических методов.

Перспективы дальнейшей работы связаны с исследованием криптографической стойкости шифровальной машины «Энигма». В частности, планируется проведение анализа устойчивости модели к современным методам криптоанализа. Это позволит оценить, насколько эффективны методы шифрования «Энигмы» в условиях современных технологий, и выявить потенциальные уязвимости, которые могут быть полезны для разработки более надёжных криптографических систем в будущем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Арзиев А.Т., Шаназаров Б. Криптографический метод шифрования и дешифрования информации на основе алгоритма машины энигма // Universum технические науки. 2024. № 4-1 (121). С. 33-35.
2. Аганин Е.И., Малышева Е.Ю. В сборнике: Начало Великой Отечественной войны: уроки истории. Взгляд из XXI века. // Материалы Международной научно-практической конференции с участием студентов. Составители Л.П. Гордеева, И.П. Ветюгова. 2016. С. 4-6.
3. Точилкин М.В. Шифрование Энигмой как один из исторических этапов развития криптографии // Студенческая наука: современные реалии. Сборник материалов III Международной студенческой научно-практической конференции. Редколлегия: О.Н. Широков [и др.]. 2017. С. 24-26.
4. Ларин Д.А., Шанкин Г.П. Вторая мировая война в эфире: некоторые аспекты операции "Ультра" // Защита информации. Инсайд. 2007. № 1 (13). С. 91-96.
5. Воронина Е.Д., Хахина А.М. Знаменитая Enigma // Наука, образование, инновации: гуманитарные, естественно-научные и технические решения современности. Материалы XXIII Всероссийской научно-практической конференции. 2020. С. 32-34.
6. Зюзин В.Д., Коробов А.В., Лопухов Р.С. Шифрование Enigma // NovaUm.Ru. 2020. № 26. С. 17-21.
7. Давлетбердин А.С., Хисаметдинов Ф.З. Шифровальная машина Enigma. // Неделя науки и технологий. Материалы всероссийской научно-практической конференции с международным участием. Сибай, 2021. С. 230-232.
8. Надточеев Е.В., Голиков А.Е. Взлом "Энигмы": спецслужбы СССР, США, Великобритании в добывании разведывательной информации в годы второй мировой войны // Государство, общество и органы внутренних дел в годы Великой Отечественной войны (1941-1945). Сборник материалов Всероссийской научно-практической конференции преподавателей, адъюнктов, курсантов, слушателей и студентов. 2015. С. 125-131.
9. Стручков И.В., Джамиев Н.М.Д., Гусева Л.Л. Анализ алгоритма работы и причин взлома шифровальной машины "Энигма" // Студенческая наука для развития информационного общества. Сборник материалов V Всероссийской научно-технической конференции: в 2 частях. 2016. С. 362-365.
10. Чепур Б. "Энигма": исторические аспекты возникновения, применение и дешифровки. Тайная спецоперация "Ультра" // Гилея: научный вестник. 2015. № 96. С. 89-93.

11. Мажей Я.В. Шифрование // Инновации. Наука. Образование. 2021. № 46. С. 1043-1048.

12. Перекатова А.Д., Горшкова Т.В. Таинственные страницы истории: криптография вчера и сегодня // Вестник науки. 2019. Т. 1. № 7 (15). С. 37-50.

REFERENCES

1. Arziev A.T., Shanazarov B. Cryptographic Method of Encryption and Decryption Based on the Enigma Machine Algorithm. *Universum Technical Sciences*. 2024. No. 4-1 (121). P. 33-35.

2. Aganin E.I., Malycheva E.Yu. In the collection: The Beginning of the Great Patriotic War: Lessons of History. A View from the 21st Century. *Materials of the International Scientific and Practical Conference with Student Participation. Compilers L.P. Gordeeva, I.P. Vetyugova*. 2016. P. 4-6.

3. Tochilkin M.V. In the collection: Student Science: Modern Realities. *Proceedings of the III International Student Scientific and Practical Conference. Editorial Board: O.N. Shirokov* [et al.]. 2017. P. 24-26.

4. Larin D.A., Shankin G.P. Information Protection. *Inside*. 2007. No. 1 (13). P. 91-96.

5. Voronina E.D., Khakhina A.M. The Famous Enigma: In the collection: Science, Education, Innovations: Humanitarian, Natural Science, and Technical Solutions of Modernity. // Materials of the XXIII All-Russian Scientific and Practical Conference. 2020. P. 32-34.

6. Zuyzin V.D., Korobov A.V., Lopukhov R.S. Enigma Encryption // NovaUm.Ru. 2020. No. 26. P. 17-21.

7. Davletberdin A.S., Khismatdinov F.Z. Enigma Ciphering Machine. *Science and Technology Week. Materials of the All-Russian Scientific and Practical Conference with International Participation. Sibai*, 2021. P. 230-232.

8. Nadtochiev E.V., Golikov A.E. Breaking "Enigma": Soviet, American, and British Intelligence Agencies in Acquiring Intelligence Information During World War II. *State, Society, and Internal Affairs Authorities During the Great Patriotic War (1941-1945). Proceedings of the All-Russian Scientific and Practical Conference of Teachers, Adjuncts, Cadets, Listeners, and Students*. 2015. P. 125-131.

9. Struchkov I.V., Djamiyev N.M.D., Guseva L.L. Analysis of the Working Algorithm and Causes of the Enigma Cipher Machine's Breakthrough. *Student Science for the Development of the Information Society. Proceedings of the V All-Russian Scientific and Technical Conference: in 2 parts*. 2016. P. 362-365.

10. Chepur B. "Enigma": Historical Aspects of Its Origin, Application, and Decryption. The Secret Operation "Ultra". *Gileya: Scientific Herald*. 2015. No. 96. P. 89-93.

11. Mazhey Y.V. Encryption. *Innovations. Science. Education*. 2021. No. 46. P. 1043-1048.

12. Perekatova A.D., Gorshkova T.V. Mysterious Pages of History: Cryptography Yesterday and Today. *Bulletin of Science*. 2019. Vol. 1. No. 7 (15). P. 37-50.

Информация об авторах

Кашковский Виктор Владимирович-д.т.н., профессор кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: viktor.kashkovskij@mail.ru

Бухаров Даниил Владимирович - магистрант кафедры информационных систем и защиты информации, Иркутский государственный университет путей сообщения (ИрГУПС, 664074, г. Иркутск, ул. Чернышевского, д. 15), e-mail: cfelpson@gmail.com

Information about the authors

Kashkovsky Viktor Vladimirovich-Doctor of Technical Sciences, Professor of the Depart-ment «Information Systems and Information Protection», Irkutsk State Transport University, Ir-kutsk, e-mail: viktor.kashkovskij@mail.ru

Bukharov Daniil Vladimirovich - undergraduate student of the Department of Information systems and information protection, Irkutsk State Transport University (IrGUPS, Russia, 664074, Irkutsk, ul. Chernyshevskogo, d. 15), e-mail: cfelpson@gmail.com