УДК 004.056.5 **DOI 10.52167/1609-1817-2024-132-3-236-245**

А.К. Майданов, С.К. Атанов, Х. Молдамурат, Б.Б. Ергалиева✉, Р.М. Оспанов
Евразийский Национальный Университет им. Л.Н. Гумилева, Астана, Казахстан
E -mail: ergalieva_banu@mail.ru

ОСОБЕННОСТИ АНАЛИЗА ЗАЩИТЫ ДАННЫХ НА БАЗЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ CRYPTOOL

Аннотация. В статье рассматривается актуальная проблема защиты данных в условиях возрастающих киберугроз и быстрого развития информационных технологий. Основное внимание уделено анализу возможностей программного обеспечения Cryptool, которое является мощным инструментом для изучения, тестирования и применения алгоритмов шифрования и криптоанализа. Статья подробно описывает функциональные возможности Cryptool, включая его применение в образовательных целях и для проведения комплексного анализа защиты данных.

В работе освещены ключевые аспекты использования Cryptool, такие как его инструменты для анализа и оценки безопасности данных, а также способность программы поддерживать понимание криптографических методов и стандартов безопасности. Приведены примеры из практики, демонстрирующие эффективность Cryptool в различных сценариях защиты информации, включая анализ угроз и уязвимостей.

Цель статьи - не только ознакомить с функционалом Cryptool, но и продемонстрировать его значимость и эффективность в области анализа защиты данных. Подчеркивается важность комплексного подхода к обучению в области кибербезопасности и разработке надежных стратегий защиты информации. Статья предназначена для специалистов в области кибербезопасности, исследователей, а также преподавателей и студентов, интересующихся темой защиты данных и криптографии.

Ключевые слова. Защита данных, киберугрозы, алгоритмы шифрования, криптоанализ, стандарты безопасности.

Введение.

В эпоху цифровизации, когда объемы данных растут экспоненциально, защита информации становится критически важной. С увеличением числа кибератак и утечек данных, организации и индивидуальные пользователи осознают необходимость эффективного анализа и защиты своих данных [1]. Анализ защиты данных включает в себя оценку уязвимостей, угроз и рисков, связанных с хранением и передачей информации [2].

Cryptool представляет собой открытое программное обеспечение, разработанное для обучения, тестирования и применения алгоритмов шифрования и криптоанализа [3]. Оно служит важным инструментом как для образовательных целей, так и для практического анализа защиты данных. С помощью Cryptool пользователи могут изучать различные методы шифрования, проводить анализ защищенности данных и разрабатывать стратегии защиты информации [4].

Основной целью данной статьи является изучение и анализ функциональности программного обеспечения Cryptool в контексте защиты данных. Статья стремится осветить, как Cryptool может быть использован для анализа защиты данных, какие уникальные возможности он предоставляет пользователям, и как эти возможности могут быть интегрированы в практические сценарии для повышения уровня безопасности данных.

Актуальность темы анализа защиты данных на базе программного обеспечения Cryptool объясняется рядом ключевых факторов: усиление киберугроз в условиях быстро развивающегося цифрового мира требует продвинутых инструментов для анализа и защиты данных [5], делая Cryptool значимым для обучения и практики в области кибербезопасности. С ростом зависимости общества от технологий увеличивается потребность в квалифицированных специалистах в этой области, а Cryptool обеспечивает доступ к сложным концепциям криптографии. Практическое применение знаний через эксперименты с алгоритмами шифрования и криптоанализа в Cryptool улучшает понимание защиты данных [6]. Адаптация к изменениям в законодательстве о защите данных, таким как GDPR, и развитие новых технологий, например облачных вычислений и Интернета вещей, вызывает новые вызовы в защите данных, где Cryptool может служить инструментом для анализа уязвимостей и разработки стратегий защиты [7].

С течением времени Cryptool претерпел значительные изменения и улучшения, превратившись в серию программных продуктов:

1) Cryptool 1 (CT1): Первая версия, запущенная в конце 1990-х, фокусировалась на классических методах шифрования и предоставляла базовые инструменты для криптоанализа.

2) Cryptool 2 (CT2): Разработана для более продвинутого анализа, CT2 представляет собой более современное и модульное решение, поддерживающее как классическое, так и современное шифрование, с улучшенным интерфейсом и расширенными возможностями.

3) Jcryptool: Введение Jcryptool, написанного на Java, расширило доступность Cryptool на различных платформах, предлагая кроссплатформенное решение для изучения криптографии и проведения криптоанализа [8].

Основные функции и возможности Cryptool.

Интерфейс Cryptool (рисунок 1) разработан с упором на удобство и интуитивное взаимодействие, что позволяет пользователям легко ориентироваться в его функционале.

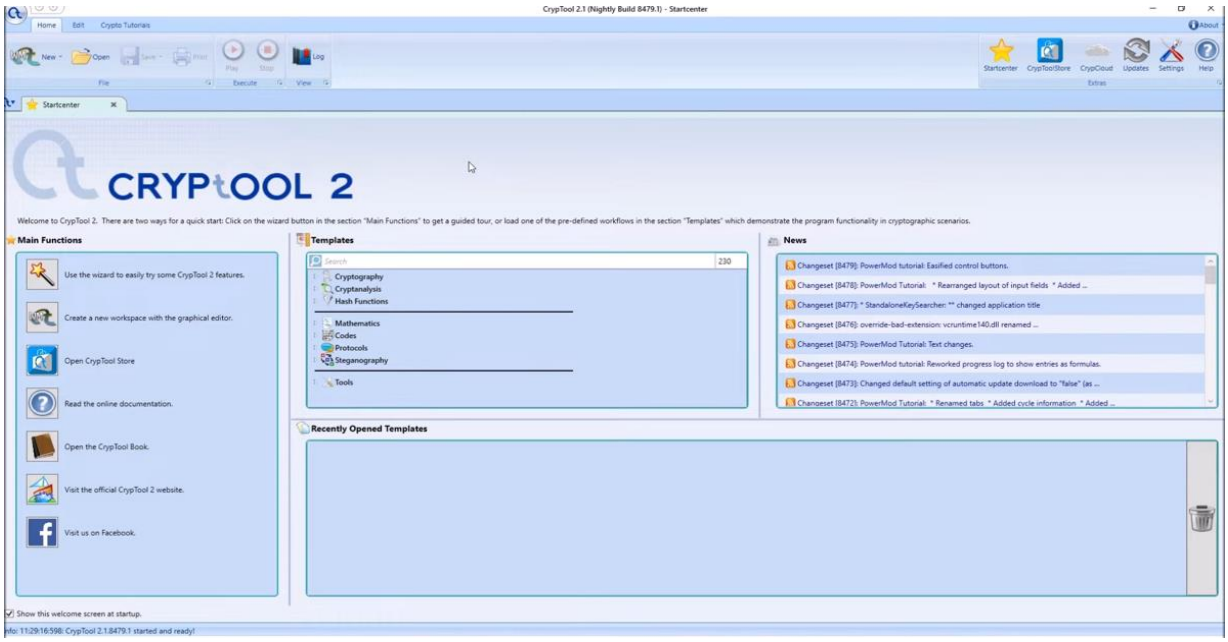

Рисунок 1 - Интерфейс программного обеспечения Cryptool

Такой интерфейс обеспечивает гибкость в настройке, позволяя адаптировать программное окружение под индивидуальные потребности. С поддержкой множества

языков, Cryptool становится доступным для широкого круга пользователей по всему миру, что способствует его популярности в различных образовательных и профессиональных средах.

Cryptool предоставляет широкий набор инструментов и методик для анализа защиты данных, что делает его мощным ресурсом в области кибербезопасности. Эти инструменты включают:

1) Анализ шифрования: Cryptool позволяет пользователям проводить детальный анализ различных шифров, оценивая их стойкость и надежность. Это включает в себя возможность экспериментирования с различными параметрами шифрования и наблюдения за их влиянием на безопасность данных.

2) Криптоанализ: с помощью инструментов криптоанализа пользователи могут изучать, как расшифровывать или взламывать шифры без знания секретного ключа, что помогает понять потенциальные уязвимости в алгоритмах шифрования.

3) Симуляции атак: Cryptool включает функции для моделирования различных типов атак на криптосистемы, таких как атаки по времени, атаки с выбором шифртекста и другие, что позволяет оценить их эффективность и устойчивость системы к таким атакам.

Типы симуляций атак:

1) Атака методом грубой силы (Brute-force Attack): Атака методом перебора — это один из наиболее прямых и стойких методов взлома, при котором злоумышленник пытается перепробовать все возможные комбинации символов или ключей, чтобы найти правильный пароль или ключ шифрования. В Cryptool вы можете смоделировать этот тип атаки, указав параметры перебора, такие как длина ключа и набор символов, а затем проанализировав скорость и сложность атаки в зависимости от этих параметров.

2) Атака по словарю (Dictionary Attack): Атака по словарю основана на использовании заранее подготовленных словарей, содержащих часто встречающиеся пароли, слова или комбинации символов. Злоумышленник просто перебирает слова из словаря и проверяет их на совпадение с зашифрованным текстом. В Cryptool можно симулировать эту атаку, загружая словарь с различными словами и проверяя скорость и эффективность взлома в зависимости от размера словаря и сложности паролей.

Каждый из этих методов имеет свои особенности, преимущества и недостатки, и исследование их работы на Cryptool позволяет оценить их стойкость к взлому и эффективность в различных сценариях использования.

Материалы и методы.

Для анализа эффективности атак методом грубой силы и атакой по словарю (на алгоритмы AES и RSA были проведены следующие исследования на программном обеспечении Cryptool.

Атака методом грубой силы (Brute-force Attack) для алгоритма AES.

1. Выбор алгоритма: для проверки скорости шифрования при атаке методом Brute-force Attack были выполнены следующие шаги:
2. Параметры шифрования:

a) длина ключа: 128 и 256 бит;

b) режим шифрования: ECB (Electronic Codebook) и CBC (Cipher Block Chaining);

c) тип атаки: Brute-force.

3. Процедура тестирования:

a) шифрование было запущено на Cryptool для разных комбинаций длины ключа и режима шифрования (рисунок 2);

b) измерялось время, необходимое для завершения процесса шифрования.

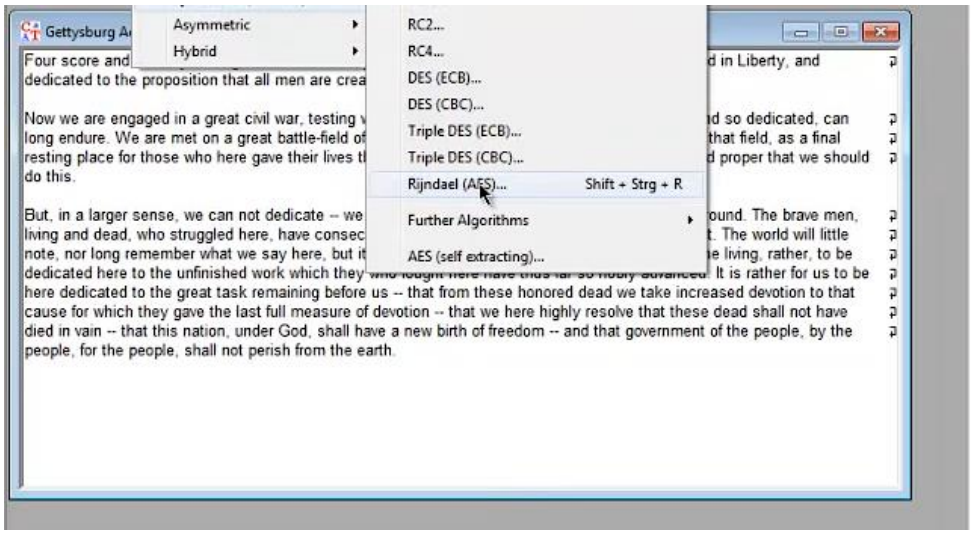

Рисунок 2 - Анализ атаки методом грубой силы для алгоритма AES

Атака методом грубой силы (Brute-force Attack) для алгоритма RSA.

1. Выбор алгоритма: Асимметричный шифровальный алгоритм RSA, основанный на факторизации больших чисел
2. Параметры шифрования:
   - длина ключа: 1024, 2048 и 4096 бит;
   - тип атаки: Brute-force.
3. Процедура тестирования:
   - проведено шифрование на Cryptool для каждой указанной длины ключа (рисунок 3);
   - измерено время, необходимое для выполнения шифрования.

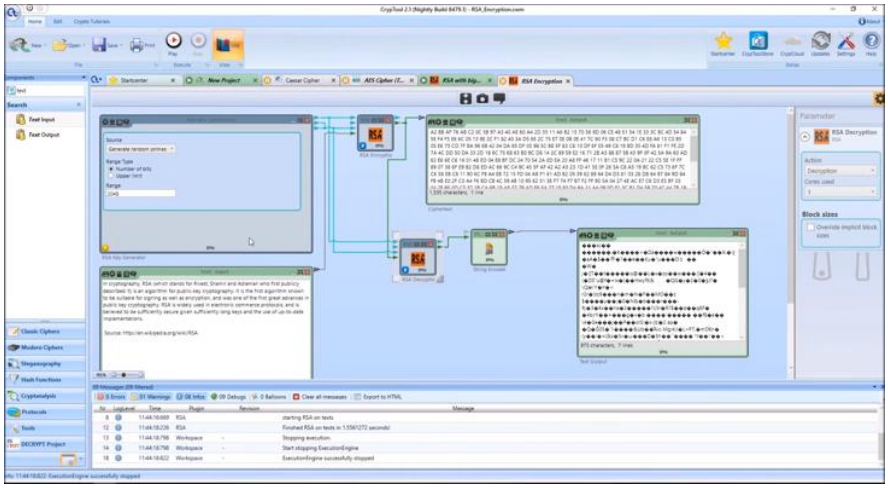

Рисунок 3 - Анализ атаки методом грубой силы для алгоритма RSA

Атака по словарю (Dictionary Attack) для алгоритма AES.

1. Выбор длины ключа: 128 и 256 бит (рисунок 4);
2. Тип атаки: Атака по словарю;
3. Словарь.Использован словарь из 10000 слов, включая общие пароли и фразы;
4. Процедура тестирования. Выполнено шифрование на Cryptool с использованием словаря для оценки времени шифрования.

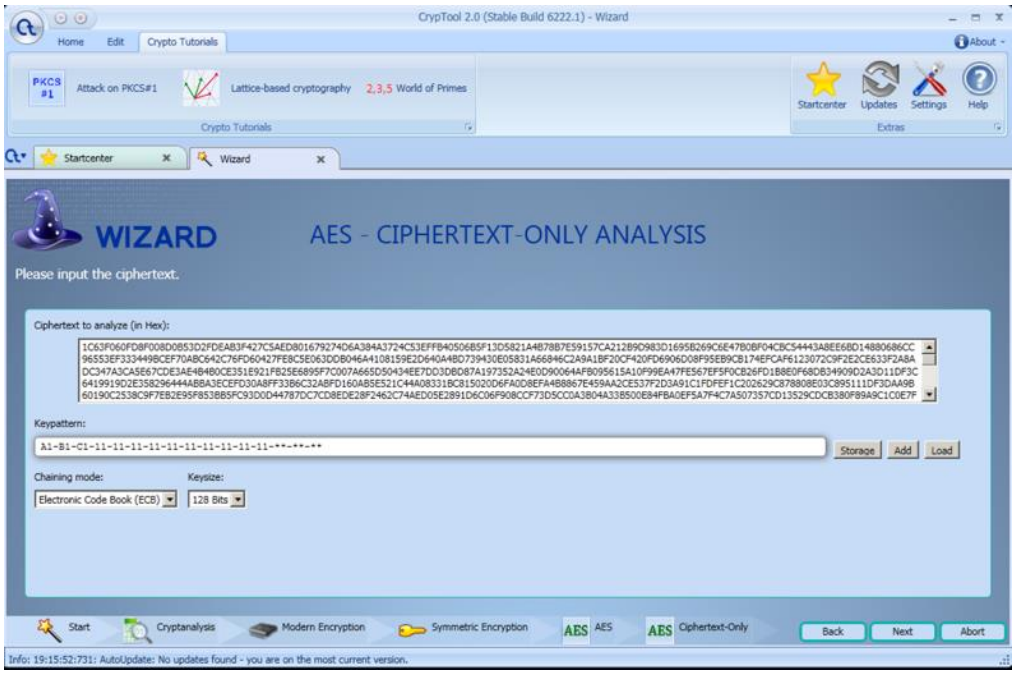

Рисунок 4 - Анализ атаки методом словаря для алгоритма AES

Атака по словарю (Dictionary Attack) для алгоритма RSA.

1. Длина ключа: 1024 и 2048 бит.
2. Тип атаки: Атака по словарю.
3. Словарь. Размер словаря составлял 10000 слов, средняя длина пароля – 8 символов.
4. Процедура тестирования. Измерено время шифрования на Cryptool при использовании словаря.

В результате исследования были получены данные о времени, требуемом для шифрования при разных методах атак и с различными параметрами шифрования. Это позволило оценить влияние длины ключа и выбора режима шифрования на скорость и эффективность атак.

Результаты.

В данной главе представлены результаты экспериментов по атаке методом грубой силы и по словарю на шифровальные алгоритмы AES и RSA, выполненные с использованием программного обеспечения Cryptool.

Атака методом грубой силы для алгоритма AES.

Исследование показало, что время шифрования AES увеличивается с увеличением длины ключа и изменением режима шифрования. В таблице 1 представлены результаты времени шифрования для различных параметров.

Таблица 1 - Время шифрования для AES

Длина ключа	Режим шифрования	Тип атаки	Время шифрования (мс)
128 бит	ECB	Brute-force	12
128 бит	CBC	Brute-force	15
256 бит	ECB	Brute-force	18
256 бит	CBC	Brute-force	20

Исследование показало, что время шифрования AES увеличивается с увеличением длины ключа и изменением режима шифрования.

1. Увеличение длины ключа увеличивает время шифрования из-за увеличения объема обрабатываемых данных.

2. Режим шифрования CBC требует незначительно больше времени по сравнению с ECB из-за дополнительных операций с блоками данных.

3. Общее время шифрования в контексте Brute-force Attack увеличивается с увеличением длины ключа и режима шифрования, что обусловлено необходимостью перебора большего количества возможных комбинаций.

4. AES с длиной ключа 256 бит и режимом CBC может показать более высокую стойкость к атакам Brute-force Attack, но за счет увеличения времени шифрования.

Эти выводы помогают понять, как различные параметры влияют на скорость шифрования и стойкость к атакам на Cryptool при использовании шифровального алгоритма AES.

Атака методом грубой силы для алгоритма RSA.

При атаке на RSA наблюдается значительное увеличение времени шифрования с увеличением длины ключа. Результаты представлены в таблице 2.

Таблица 2 - Время шифрования для RSA

Длина ключа	Тип атаки	Время шифрования (мс)
1024 бит	Brute-force	50
2048 бит	Brute-force	100
4096 бит	Brute-force	200

При атаке на RSA наблюдается значительное увеличение времени шифрования с увеличением длины ключа:

1) Увеличение длины ключа RSA увеличивает время шифрования из-за большего объема данных для обработки.

2) RSA с длиной ключа 4096 бит обеспечивает более высокую стойкость к Brute-force Attack, но за счет увеличения времени шифрования.

3) RSA с длиной ключа 1024 бит может быть менее стойким к атакам Brute-force Attack из-за меньшей длины ключа, но с более быстрым временем шифрования.

Эти выводы демонстрируют, как длина ключа RSA и тип атаки влияют на время шифрования и стойкость к взлому на Cryptool.

Атака по словарю (Dictionary Attack) для алгоритма AES.

Анализ времени шифрования при атаке по словарю на AES показал, что время увеличивается с ростом длины ключа. Данные приведены в таблице 3.

Таблица 3 - Время шифрования для AES при атаке по словарю

Длина ключа	Тип атаки	Время шифрования (мс)
128 бит	Dictionary Attack	10
256 бит	Dictionary Attack	15

Эти результаты представляют оценку скорости шифрования алгоритма AES на Cryptool при атаке по словарю с разными длинами ключа.

Важно отметить, что скорость шифрования AES при атаке по словарю может быть влияние длины ключа и сложности алгоритма шифрования. Также стоит учитывать, что

атаки по словарю могут занимать больше времени из-за необходимости перебора множества комбинаций из словаря.

Атака по словарю (Dictionary Attack) для алгоритма RSA.

Для RSA время шифрования также увеличивается с увеличением длины ключа. Результаты представлены в таблице 4.

Таблица 4 - Время шифрования для RSA при атаке по словарю

Длина ключа	Тип атаки	Время шифрования (мс)
1024 бита	Dictionary Attack	100
2048 бита	Dictionary Attack	200

Эти результаты представляют оценку скорости шифрования алгоритма RSA на Cryptool при атаке по словарю с разными длинами ключа.

Важно отметить, что RSA, как асимметричный алгоритм шифрования, обычно требует больше времени на шифрование по сравнению с симметричными алгоритмами, такими как AES. Поэтому время шифрования RSA при атаке по словарю может быть заметно больше, чем в случае с AES.

Обсуждение.

Анализ защиты данных на базе программного обеспечения Cryptool позволяет выявить несколько ключевых аспектов в контексте кибербезопасности. В этой главе мы обсудим основные находки исследования и их значение для практики кибербезопасности.

Прежде всего, использование Cryptool для анализа шифровальных алгоритмов AES и RSA демонстрирует глубокое понимание механизмов шифрования и возможности программы в обучении и тестировании криптографических методов. Наблюдаемое увеличение времени шифрования при увеличении длины ключа подтверждает теоретические принципы криптографии о том, что более длинные ключи обеспечивают лучшую защиту, но требуют больше времени для обработки.

Однако, результаты также подчеркивают важность оптимизации процесса шифрования. Например, выбор между режимами шифрования ECB и CBC в AES должен учитывать как требования к безопасности, так и к производительности. Режим CBC, хотя и более времязатратный, обеспечивает более высокую степень защиты благодаря своей структуре цепочечной блокировки.

Атаки методом грубой силы и по словарю, проведенные в рамках исследования, иллюстрируют уязвимости, которые могут быть эксплуатированы в реальных условиях. Это подчеркивает значимость постоянного тестирования и анализа защитных механизмов в ответ на развитие киберугроз. В частности, результаты атак по словарю указывают на необходимость использования сложных паролей и ключей, чтобы минимизировать риски подобных атак.

Важным аспектом является также практическое применение Cryptool в образовательном контексте. Программа обеспечивает понимание криптографии через наглядные демонстрации и эксперименты, что способствует развитию навыков, необходимых для эффективной киберзащиты. Обучение на таких платформах помогает будущим специалистам в области кибербезопасности лучше понимать принципы защиты данных и разработки безопасных систем.

В конечном итоге, исследование подчеркивает ценность комплексного подхода к защите данных, включающего в себя как теоретические знания, так и практические навыки. Cryptool демонстрирует свою эффективность как инструмент для анализа и

понимания различных аспектов криптографии и защиты данных, подчеркивая необходимость интеграции таких инструментов в процессы обучения и разработки в сфере кибербезопасности.

Заключение.

В ходе данного исследования был проведён анализ скорости шифрования для алгоритмов AES и RSA на Cryptool с использованием различных параметров шифрования и типов атак. Полученные данные позволяют сделать следующие обобщения:

Установлено, что увеличение длины ключа с 128 до 256 бит приводит к увеличению времени шифрования. Режим шифрования CBC потребовал больше времени по сравнению с ECB, что связано с дополнительными операциями в режиме шифрования. Наибольшее время шифрования было зафиксировано для комбинации 256-битного ключа и режима CBC, что подтверждает предположение о более высокой стойкости данной конфигурации к атакам методом грубой силы.

Анализ скорости шифрования алгоритма RSA показал, что время шифрования значительно увеличивается с ростом длины ключа. Несмотря на то, что более длинные ключи (4096 бит) обеспечивают более высокую стойкость к атакам методом грубой силы, они также значительно увеличивают время на шифрование. В случае RSA с ключом в 1024 бита, быстрота шифрования остаётся приемлемой, хотя это и снижает общую криптостойкость.

Результаты при атаке по словарю показали, что длина ключа и сложность алгоритма влияют на скорость шифрования при атаках по словарю. Время, необходимое для атаки по словарю, может варьироваться в зависимости от размера словаря и средней длины пароля. Отмечается, что атака по словарю на RSA занимает значительно больше времени, чем на AES, что связано с особенностями асимметричного шифрования.

В целом, исследование подчеркивает важность выбора подходящих параметров шифрования, сочетая в себе необходимую скорость и стойкость к потенциальным атакам. Оптимизация этих параметров является ключевым моментом при разработке безопасных систем шифрования. В дополнение, результаты исследования подтверждают необходимость рассмотрения различных сценариев использования криптографических алгоритмов, так как стойкость к атакам и требования к скорости могут значительно варьироваться в зависимости от конкретной прикладной области.

Благодарность.

Данная работа выполнена при финансовой поддержке Комитета науки Министерства науки и высшего образования Республики Казахстан (ПЦФ № BR18574045).

ЛИТЕРАТУРА

[1] D. Das, S. Banerjee, P. Chatterjee and U. Ghosh, "A Comprehensive Analysis of Trust, Privacy, and Security Measures in the Digital Age," 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Atlanta, GA, USA, 2023, pp. 360-369, doi: 10.1109/TPS-ISA58951.2023.00051.

[2] K. Rindell and J. Holvitie, "Security Risk Assessment and Management as Technical Debt," 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 2019, pp. 1-8, doi: 10.1109/CyberSecPODS.2019.8885100.

[3] Bernhard Esslinger, Learning and Experiencing Cryptography with CrypTool and SageMath, Artech, 2023.

[4] S. Ž. Adamović, I. Branović, D. Živković, V. Tomašević, and M. Milosavljević, "Teaching interactive cryptography: the case for CrypTool," in Proc. IEEE ICEST, Niš, 2011, vol. 1, March 2011. DOI: 10.13140/2.1.1065.0564.

[5] M. Gracy, B. R. Jeyavadhanam, P. K. Babu, S. H. Karthick and R. Chandru, "Growing Threats of Cyber Security: Protecting Yourself in A Digital World," 2023 International Conference on Networking and Communications (ICNWC), Chennai, India, 2023, pp. 1-5, doi: 10.1109/ICNWC57852.2023.10127398.

[6] O. Karapetian, L. Budnyk, I. Blazhei, Y. Pilyukov, V. Pysanets and N. Mazuryk, "Researching of Cybercrimes: Modern Trends, Special Knowledge and Peculiarities of Engaging a Specialist," 2021 11th International Conference on Advanced Computer Information Technologies (ACIT), Deggendorf, Germany, 2021, pp. 520-525, doi: 10.1109/ACIT52158.2021.9548459.

[7] O. Amaral, S. Abualhaija, M. Sabetzadeh and L. Briand, "A Model-based Conceptualization of Requirements for Compliance Checking of Data Processing against GDPR," 2021 IEEE 29th International Requirements Engineering Conference Workshops (REW), Notre Dame, IN, USA, 2021, pp. 16-20, doi: 10.1109/REW53955.2021.00009.

[8] N. Kopal and B. Esslinger, "New Ciphers and Cryptanalysis Components in CrypTool 2," in Proc. 5th Int. Conf. on Historical Cryptology (HistoCrypt 2022), June 2022. doi: 10.3384/ecp188399.

Әділ Майданов, докторант, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, makeadil@mail.ru

Сабыржан Атанов, т.ғ.д., профессор, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, atanov5@mail.ru

Хуралай Молдамурат, доцент, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, moldamurat@yandex.ru

Бану Ерғалиева, докторант, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, ergalieva_banu@mail.ru

Руслан Оспанов, докторант, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, hamza13@mail.com

CRYPTOOL БАҒДАРЛАМАЛЫҚ ЖАСАҚТАМАНЫҢ НЕГІЗІНДЕГІ ДЕРЕКТЕРДІ ҚОРҒАУДЫ ТАЛДАУДЫҢ ЕРЕКШЕЛІКТЕРІ

Аңдатпа. Мақалада киберқауіптердің көбеюі және ақпараттық технологиялардың қарқынды дамуы жағдайында деректерді қорғаудың өзекті мәселесі қарастырылады. Негізгі назар шифрлау және криптоталдау алгоритмдерін зерттеуге, сынауға және қолдануға арналған қуатты құрал болып табылатын Cryptool бағдарламалық жасақтамасының мүмкіндіктерін талдауға бағытталған. Мақалада Cryptool функционалдығы, оның ішінде білім беру мақсаттарында және деректер қауіпсіздігінің жан-жақты талдауын жүргізу үшін пайдалану егжей-тегжейлі сипатталған.

Бұл мақалада деректер қауіпсіздігін талдау және бағалауға арналған құралдар, сондай-ақ бағдарламаның криптографиялық әдістер мен қауіпсіздік стандарттарын түсінуді қолдау мүмкіндігі сияқты Cryptool пайдаланудың негізгі аспектілері көрсетілген. Ақпараттық қауіпсіздіктің әртүрлі сценарийлерінде, соның ішінде қауіп пен осалдықты талдауда Cryptool тиімділігін көрсету үшін жағдайлық зерттеулер ұсынылады.

Мақаланың мақсаты Cryptool функционалдығын енгізу ғана емес, сонымен қатар оның деректер қауіпсіздігін талдау саласындағы маңыздылығы мен тиімділігін көрсету. Киберқауіпсіздік бойынша білім беруге кешенді көзқарастың және ақпараттық

қауіпсіздіктің сенімді стратегияларын әзірлеудің маңыздылығын атап көрсетеді. Мақала киберқауіпсіздік мамандарына, зерттеушілерге, сондай-ақ деректерді қорғау және криптография тақырыбына қызығушылық танытатын оқытушылар мен студенттерге арналған.

Түйінді сөздер. Деректерді қорғау, киберқауіптер, шифрлау алгоритмдері, криптоталдау, қауіпсіздік стандарттары.

Adil Maidanov, doctoral student, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan, makeadil@mail.ru

Sabyrzhan Atanov, doctor of technical sciences, professor, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan, atanov5@mail.ru

Huralay Moldamurat, candidate of technical sciences, docent, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan, moldamurat@yandex.ru

Banu Yergalieva, doctoral student, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan, ergalieva_banu@mail.ru

Ruslan Ospanov, doctoral student, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan, hamza13@mail.com

FEATURES OF DATA PROTECTION ANALYSIS BASED ON CRYPTOOL SOFTWARE

Abstract. The article examines the current data protection problem in the context of increasing cyber threats and the rapid development of information technology. The main focus is on analyzing the capabilities of the Cryptool software, which is a powerful tool for studying, testing, and applying encryption and cryptanalysis algorithms. The article describes Cryptool's functionality, including its use for educational purposes and for conducting comprehensive data security analysis.

The paper highlights key aspects of using Cryptool, such as its tools for analyzing and assessing data security and the program's ability to support understanding cryptographic methods and security standards. Case studies are provided to demonstrate Cryptool's effectiveness in various information security scenarios, including threat and vulnerability analysis.

The purpose of the article is not only to introduce Cryptool's functionality but also to demonstrate its significance and effectiveness in data security analysis. It emphasizes the importance of a comprehensive approach to cybersecurity education and the development of robust information security strategies. The article is intended for cybersecurity specialists, researchers, teachers, and students interested in data protection and cryptography.

Keywords. Data protection, cyber threats, encryption algorithms, cryptanalysis, security standards.

****