УДК 004.056

МОДЕЛИРОВАНИЕ АТАКИ ПЕРЕБОРА ПАРОЛЕЙ И ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ МЕХАНИЗМОВ ЗАЩИТЫ СИСТЕМЫ АУТЕНТИФИКАЦИИ

Иванов М.Д., студент гр. ИБт-231, III курс
Научный руководитель: Дементьева Ю.С., преподаватель кафедры ИБ
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово

Чем глубже мы погружаемся в цифровую среду, тем больше учётных записей вынуждены создавать: социальные сети, государственные порталы, банковские приложения. Каждый из аккаунтов требует пароля, и с ростом их количества пользователю становится сложнее придумывать и запоминать уникальные комбинации. Как следствие, люди прибегают к повторному использованию паролей или минимальной модификации их для разных сервисов. Такая стратегия создаёт уязвимость, при которой в случае утечке базы данных одного из сервисов злоумышленник может получить доступ к другим аккаунтам пользователя.

Наиболее прямым методом эксплуатации данной уязвимости является атака перебора паролей (brute-force). Брутфорс – это перебор всевозможных значений уникального поля данных для конкретного пользователя, которым интересуется злоумышленник. Подобрав нужное значение, злоумышленник получает доступ к личным данным, которыми он может воспользоваться в своих личных интересах [1, с. 522]. В условиях отсутствия защитных механизмов даже пароль средней сложности может быть подобран за приемлемое для атакующего время.

В то же время, в арсенале специалистов по кибербезопасности существует ряд механизмов, способных существенно затруднить или вовсе остановить атаку перебором: ограничение количества попыток входа, временные задержки, блокировка учётной записи, использование CAPTCHA. Однако эффективность каждого из этих методов сильно зависит от контекста реализации и параметров атаки, что требует проверки в контролируемых условиях, например, моделирование системы аутентификации с возможностью выборочного ручного включения механизмов защиты с возможностью фиксации результатов в отдельное поле.

Актуальность темы обусловлена необходимостью опытной оценки эффективности механизмов защиты от атак перебора паролей. Существующие исследования часто носят теоретический характер или фокусируются на отдельных аспектах защиты, тогда как цельное сравнение методов в рамках

единой программной модели позволяет получить более объективные данные для принятия проектных решений при разработке систем аутентификации.

Цель работы: исследование эффективности механизмов защиты системы аутентификации от атак перебора паролей с помощью программного моделирования.

Задачи:

1. Проанализировать теоретические основы угроз атак перебора паролей, а также систематизировать существующие механизмы защиты систем аутентификации.
2. Разработать программную модель системы аутентификации с интегрированным модулем для имитации атаки перебора и возможностью гибкой настройки механизмов защиты.
3. Провести серию экспериментов для оценки времени подбора пароля при различных конфигурациях защиты.
4. Выполнить сравнительный анализ результатов и сформулировать практические рекомендации.

В первую очередь следует определить базовые понятия, связанные с перебором паролей и системами аутентификаций. В частности, определить основные виды атак методом грубой силы, а также возможные способы защиты.

В основном выделяют 6 способов перебора пароля:

1. Глобальный (классический) перебор. Данный способ заключается в поочередной проверке всех возможных комбинаций символов. Метод гарантирует нахождение пароля при достаточном времени работы, однако эффективность метода снижается с ростом длины пароля, наличием комбинации содержащих спецсимволы и смешанный регистр.
2. Статистически оптимизированный перебор. Показатель встречаемости определенных символов в пользовательских паролях почти такой же, как и частотностью букв в естественном языке, поэтому в данном способе сначала проверяются комбинации, состоящие из наиболее вероятных символов, что позволяет сократить время на перебор по сравнению с классическим подходом. Данный метод также может использовать статистику встречаемости биграмм и триграмм (частота встречаемости последовательности символов из двух и трех символов соответственно).
3. Словарная атака. Пользователи склонны выбирать осмысленные слова, например имена или даты вместо случайной последовательности символов, что позволяет злоумышленникам использовать предварительно сформированные словари. Современные словари для перебора включают наиболее распространённые пароли из утекших баз данных.
4. Персонализированный перебор. Это атака с применением методов социальной инженерии. Злоумышленник собирает открытую

информацию о жертве: имена родственников, даты, номера телефонов, затем формирует словарь для генерации паролей [2, с. 108–109].

5. Гибридная атака. Комбинирует словарный подход с грубым перебором, а именно, к словам из словаря добавляются цифры, спецсимволы и вариации регистра, например, пароль «password» в гибридном методе превращается в «Password123!». Данный метод эффективен против пользователей, которые формально соблюдают требования к сложности пароля, но сохраняют его предсказуемость.
6. Обратный перебор (Reverse brute-force). В данном способе вместо подбора пароля к известному логину, атакующий использует один распространённый пароль и перебирает список возможных логинов, однако нахождение совпадений не гарантируется.

Для противодействия перечисленным угрозам в системах аутентификации может применяться ряд механизмов защиты:

- Ограничение количества попыток ввода паролей.
- Задержка между попытками ввода.
- Использование CAPTCHA, то есть специального теста, который помогает определить кем является пользователем сайта – человек или бот.
- Блокирование аккаунта после нескольких неудачных попыток ввода [3, с.75].
- Блокировка злоумышленника по IP-адресу при выявлении подозрительной активности с адреса

Актуальность проблемы атак перебором паролей подтверждается центром исследования киберугроз Solar 4RAYS ГК «Солар» [4]. Согласно отчёту за I квартал 2025 года, brute-force атаки составили 94% всех зафиксированных событий в сети сервисов приманок (сеть ханипотов), а их количество увеличилось на 172% по сравнению с предыдущим кварталом.

Таким образом, опытная оценка эффективности механизмов борьбы с атакой перебором паролей позволит обосновать каждый механизм защиты и определить какой из них даёт наибольший прирост устойчивости при минимальных затратах, что позволит организациям выстраивать стратегию защиты в условиях роста кибератак на системы аутентификации.

В связи с этим, целью данной работы является разработка программного средства для имитации атак перебора и исследования эффективности механизмов защиты системы аутентификации. Для этого было создано C# приложение, позволяющее осуществлять словарную атаку на простейшую модель системы входа. В программе реализованы ключевые механизмы борьбы: ограничение попыток, временные задержки, блокировка учётной записи, CAPTCHA - которые могут гибко включаться и комбинироваться в ходе опытов. Результаты тестирования фиксируются в отдельном модуле в виде таблицы для последующего анализа.

Разработанное приложение состоит из четырёх функциональных модулей: аутентификация, механизмы защиты, модуль атаки и блок с результатами экспериментов. Интерфейс программы представлен на рисунке 1.

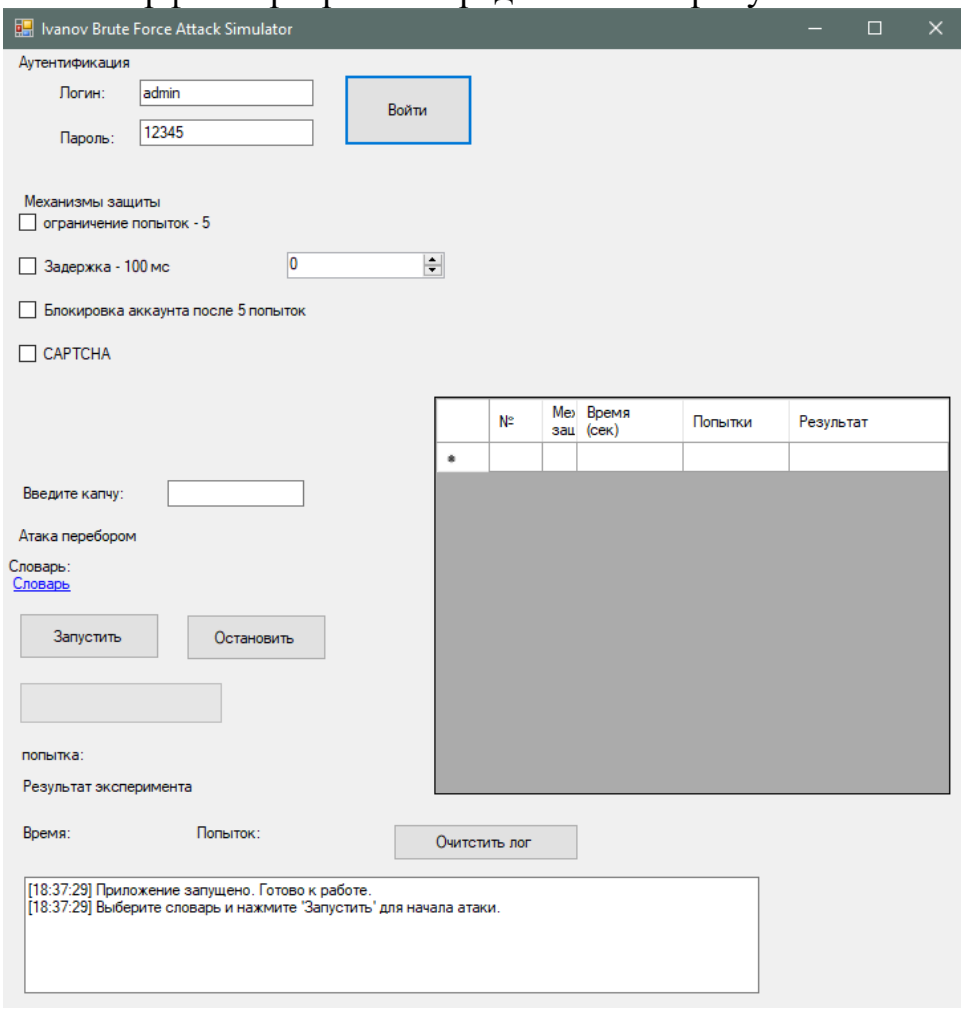

Рисунок 1 - Интерфейс программы

Приложение позволяет вручную ввести логин и пароль, по умолчанию логином является слово «admin», пароль «12345». Для исследования эффективности защиты реализованы четыре механизма, которые можно включать и выключать в произвольном порядке. Ограничение количества попыток ввода - после 5 неудачных попыток аутентификации система полностью блокирует дальнейший ввод без возможности восстановления. Временная задержка между попытками - позволяет задать интервал от 1 до 100 мс между последовательными попытками входа. Временная блокировка учётной записи - после 5 неудачных попыток аккаунт блокируется на 30 секунд, после чего счётчик попыток сбрасывается и пользователю предоставляется ещё 5 попыток. Стоит отметить, что данный метод отличается от ограничения попыток тем, что возможность ввода восстанавливается. Однако для упрощения проведения экспериментов ожидание в 30 секунд отключено для атаки перебором, каждые 5 неудачных попыток атака останавливается. CAPTCHA - механизм проверки человек/бот, который требует выполнения дополнительного теста перед аутентификацией. Во время атаки программа действительно считает пример,

изображенный на CAPTCHA, однако для отражения реальной задержки было выставлено замедление в 200 миллисекунд (имитация времени отклика сервера).

В блоке «Атака перебором» необходимо выбрать словарь, с помощью которого будет проводиться атака, словарь должен представлять собой текстовый документ с одним словом (паролем) на каждой строке. Во время атаки имеется возможность наблюдать шкалу прогресса, а также номер попытки и вводимый пароль. После завершения атаки независимо от исхода – результат вносится в специальную таблицу с номером атаки, временем продолжительности, количеством попыток, а также результатом поиска пароля. Также имеется лог, который фиксирует происходящие события, имеется возможность очистки лога.

Для оценки эффективности механизмов защиты была проведена серия экспериментов с использованием словаря, содержащего корректный пароль на 2251-й строке. В каждом эксперименте активировался один из механизмов защиты (в первом тесте защита отсутствовала). Результаты пяти тестов представлены на рисунке 2.

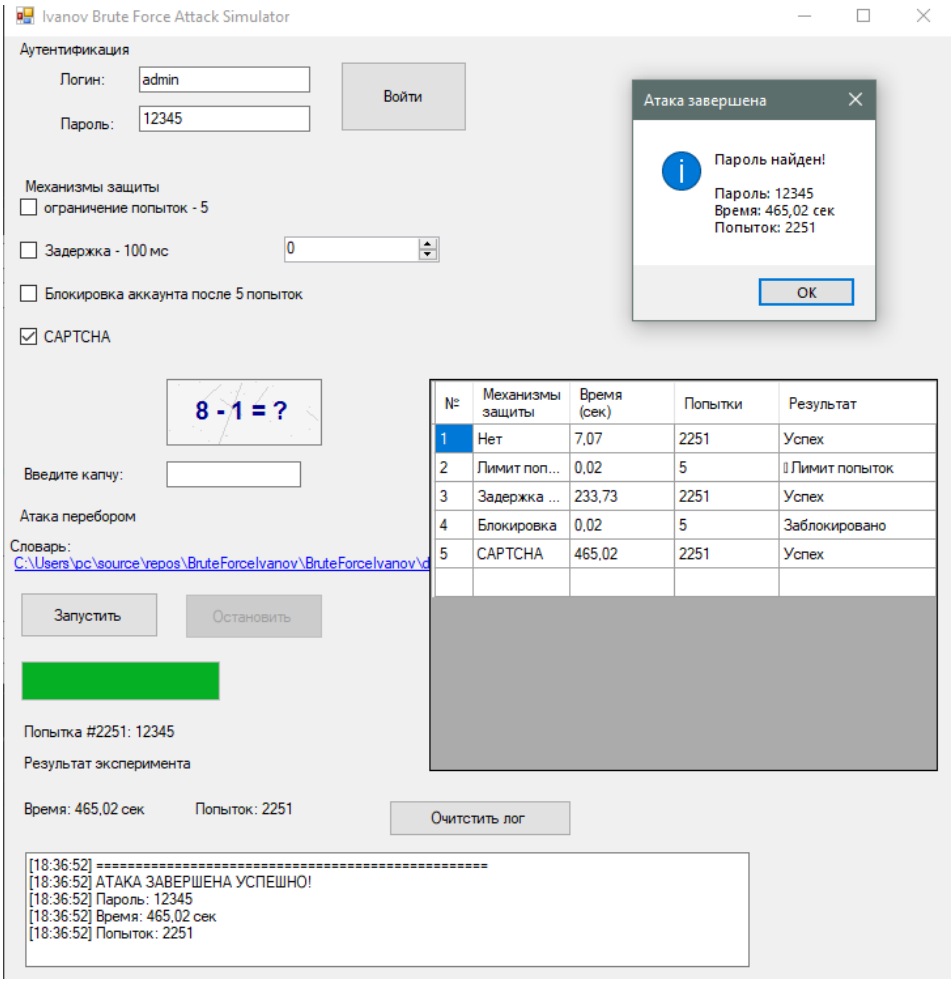

Рисунок 2 - Программа с таблицей результатов пяти экспериментов

Для наглядного сравнения эффективности механизмов защиты основные метрики экспериментов сведены в таблицу на рисунке 3.

№	Механизм защиты	Время (сек)	По-пытки	Результат	Эффектив-ность
1	Отсутствует	7,07	2251	Успешный под-бор	Не защищено
2	Ограничение попы-ток (5)	0,02	5	Блокировка	Полная за-щита
3	Задержка 100 мс	233,73	2251	Успешный под-бор	Частичная за-щита
4	Блокировка акка-унта	0,02	5	Временная бло-кировка	Полная за-щита
5	CAPTCHA	465,02	2251	Успешный под-бор	Частичная за-щита

Рисунок 3 - Таблица результатов тестирования механизмов защиты аутентификации

Ограничение попыток и блокировка аккаунта показали максимальную эффективность: атака была остановлена после 5 попыток за 0,02 секунды. Однако данные механизмы имеют принципиально разные последствия: ограничение попыток приводит к необратимой блокировке ввода, что делает систему уязвимой для DoS-атак (злоумышленник может заблокировать аккаунт легитимного пользователя), блокировка аккаунта предполагает временную изоляцию с последующим восстановлением доступа, что более безопасно для пользовательского опыта.

Временная задержка (100 мс) увеличила время атаки с 7,07 до 233,73 секунд, то есть в 33 раза, но не предотвратила успешный подбор. Данный механизм необходимо использовать как вспомогательную меру вместе с другими методами защиты.

CAPTCHA показала набольшую эффективность по времени - 465,02 секунд, но также не остановила атаку. Это объясняется тем, что в рамках моделирования CAPTCHA не создавала реальных препятствий для автоматизированного скрипта. В реальных условиях CAPTCHA эффективна против простых ботов, но специализированные сервисы распознавания способны обойди данный тест.

На основе полученных результатов можно сформулировать ряд рекомендаций по выбору механизмов защиты в зависимости от контекста использования системы аутентификации.

Для высокозащищённых системы (государственные информационные системы, банковские приложения, корпоративные ресурсы спецслужб) рекомендуется использовать ограничение попыток или блокировку аккаунта, так как защищенность системы приоритетнее удобства, стоит отметить, что необратимая блокировка допустима лишь при наличии альтернативных каналов восстановления доступа.

Массовым сервисам (социальные сети, почтовые сервисы, развлекательные платформы) следует использовать менее жесткие меры, например задержка между попытками ввода, CAPTCHA или временная блокировка аккаунта. Такой выбор поможет сервисам предотвратить атаки, нацеленные на выведение из строя серверов, замедлить атаку и отфильтровать простых ботов. В

данном случае механизмы защиты не отнимают всё удобство, а балансируют между безопасностью и пользовательским опытом.

Внутренним корпоративным системам предлагается установка таких механизмов защиты как задержка и ограничение попыток с уведомлением системного администратора. В данном случае ставка делается на ручной контроль, так как системный администратор в состоянии самостоятельно проверить каждого пользователя и осуществить разблокировку аккаунта.

Таким образом, каждый механизм защиты продемонстрировал собственную эффективность по сравнению с системой аутентификации, в которой методы борьбы с атакой перебором отсутствуют вовсе. Однако выбор должен основываться на балансе между уровнем безопасности, удобством использования и устойчивостью к атакам. Оптимальной стратегией является комбинирование нескольких механизмов.

Список литературы:

1. Колесник, Д. П. Таймингговые атаки и методы борьбы с ними / Д. П. Колесник, А. Р. Балса // Современное состояние, проблемы и перспективы развития отраслевой науки : Материалы Всероссийской конференции с международным участием, Москва, 23–24 ноября 2017 года. – Москва: Издательство "Перо", 2017. – С. 522-525. – EDN YRLBYD
2. Кузьмин, Н. И. Несанкционированный доступ с помощью прямого перебора пароля – BrutForce / Н. И. Кузьмин, Н. Н. Панкова // Научное сообщество студентов : сборник материалов XIV Международной студенческой научно-практической конференции, Чебоксары, 26 мая 2017 года. – Чебоксары: Общество с ограниченной ответственностью "Центр научного сотрудничества "Интерактив плюс", 2017. – С. 107-109. – EDN YQWTMB.
3. Речкалова, О. О. Хакеры – герои нашего времени? / О. О. Речкалова, Д. И. Шелихов // Союз криминалистов и криминологов. – 2018. – № 1. – С. 70-76. – DOI 10.31085/2310-8681-2018-1-70-76. – EDN YLLMHR.
4. Ландшафт кибератак Q1 2025: аналитика ханипотов и сенсоров. — Текст: электронный // Солар: [сайт]. — URL: https://rt-solar.ru/analytics/reports/5626/ (дата обращения: 23.03.2026).