звеном, которое соединяет технологии и человеческое восприятие, превращая стандартные рекламные форматы в оригинальные идеи, вызывающие интерес и вдохновение. Использование этого подхода позволяет создавать рекламу, которая не просто информирует, а удивляет, заставляет задуматься и запоминается надолго. Таким образом, рекламные инновации через призму латерального мышления открывают перед брендами новые горизонты – от уникальных форм коммуникации до формирования устойчивого имиджа в сознании потребителей.

Список использованных источников

1. Латеральное мышление в бизнесе: ключ к инновациям и решению сложных задач [Электронный ресурс] – Режим доступа: https://rb.ru/columns/lateralnoe-myshlenie/ Дата доступа: 11.11.2025
2. Что такое латеральное мышление [Электронный ресурс] – Режим доступа: https://blog.ikraikra.ru/chto-takoe-lateralnoe-myshlenie/ Дата доступа: 11.11.2025
3. Кузьмичева, Ю. А. Социокультурные тенденции развития рекламы в современном мире / Ю. А. Кузьмичева // Образование и наука без границ: социально-гуманитарные науки. — 2020.

УДК 681.3:553.98(574.4)

Б.А. Атаджанов, О.Д. Ныязгылыджева, М.А. Атаев, М. Чарыева
Международный университет нефти и газа имени Ягшыгельди Какаева
Ашхабад, Туркменистан
Туркменский государственный энергетический институт
Мары, Туркменистан

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ЗАЩИТЫ ОТ ДЕБАГГЕРОВ В WINDOWS-ПРИЛОЖЕНИЯХ

Аннотация. *В статье рассматривается программный подход к защите Windows-приложений от анализа и взлома с использованием отладчиков (дебаггеров). На примере простой программы демонстрируется, каким образом злоумышленник может получить доступ к строковым данным приложения посредством дизассемблирования, и предлагаются конкретные методы противодействия.*

B.A. Atajanov, O.D. Nyyazgylyjeva, M.A. Atayev, M. Charyyeva
Yagshigeldi Kakaev International Oil and Gas University
Ashgabat, Turkmenistan

Turkmen State Energy Institute
Mary, Turkmenistan

SOFTWARE PROTECTION AGAINST DEBUGGERS IN WINDOWS APPLICATIONS

Abstract. *The article describes a software method for protecting Windows applications from analysis and cracking using debuggers. A simple application demonstrates how an attacker can extract text strings through disassembly in OllyDbg. Several countermeasures are proposed: hiding sensitive strings inside GUI components, encrypting data prior to compilation, using XOR-based protection, and storing duplicate critical information in the system registry.*

Современные программные средства, особенно предназначенные для обработки конфиденциальных данных, нуждаются в защите от вмешательства и анализа со стороны злоумышленников. Одним из наиболее распространённых инструментов взлома является дебаггер — программа, позволяющая исследовать внутреннюю структуру исполняемого файла, просматривать строки, изменять значения переменных и управлять ходом выполнения.

Простой пример показывает, что даже примитивная проверка пароля, реализованная в исходном коде, может быть легко обнаружена и обойдена при помощи дебаггера. Это поднимает вопрос о необходимости применения дополнительных мер защиты в пользовательских приложениях.

Исходный пример представляет собой Windows-приложение, запрашивающее у пользователя пароль. При запуске отображается окно с полем ввода и кнопкой проверки. Правильный пароль — *“Merdan”*. В случае правильного ввода выводится сообщение «Dogry» и открывается следующее окно.

Обработчик события кнопки имеет следующий вид:

```
if edit1.Text='Merdan' then
begin
  ShowMessage('Dogry');
  Form2.Show;
end
else Close;
```

Таким образом, пароль хранится в коде в виде открытой строковой константы, что упрощает анализ.

Программа была загружена в OllyDbg через меню *File → Open*. В окне отображается дизассемблированный машинный код файла *Project1.exe*.

Для поиска строковых данных используется команда: **Search for → All referenced text strings**.

Результат показывает все строки, присутствующие в исполняемом файле, включая пароль «Merdan». Следовательно, защита

программы считается взломанной: злоумышленник легко извлекает пароль, просматривает или изменяет поведение программы (Рис. 1).

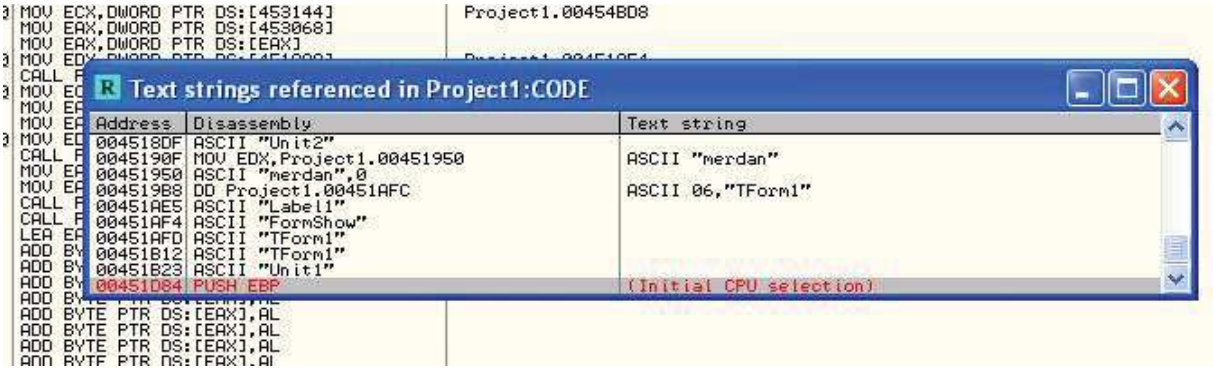

Рис 1 - Обнаружение строки, хранящей пароль в окне отладчика.

Подобный анализ выявляет уязвимость: открытое хранение строк в коде недопустимо.

Первый предлагаемый метод — скрытие строки-пароля не в коде, а в визуальном компоненте интерфейса (например, *Label1*) [1], который:

- содержит необходимую строку в свойстве *Caption*,
- невидим при запуске (*Visible = False*).

В этом случае даже при поиске строк в OllyDbg пароль не обнаруживается напрямую, поскольку он не фигурирует в виде явной строковой константы в коде программы.

Однако опытный взломщик может продолжить анализ, поэтому предлагается внедрить дополнительные уровни защиты.

1. Шифрование строк XOR-операцией

На этапе до компиляции все текстовые данные (пароли, пути, конфигурации) должны быть преобразованы XOR-шифрованием. При выполнении программы расшифровка выполняется по требованию, что делает данные нечитаемыми при статическом анализе.

2. Полный отказ от хранения чувствительных данных во внешних файлах

Все пароли и ограничительные строки должны храниться таким образом, чтобы они не находились в обычных текстовых файлах, не размещались в ресурсах и не сохранялись в отдельных конфигурационных файлах. Такой подход позволяет предотвратить их простое извлечение и обеспечивает более высокий уровень безопасности (Рис. 2).

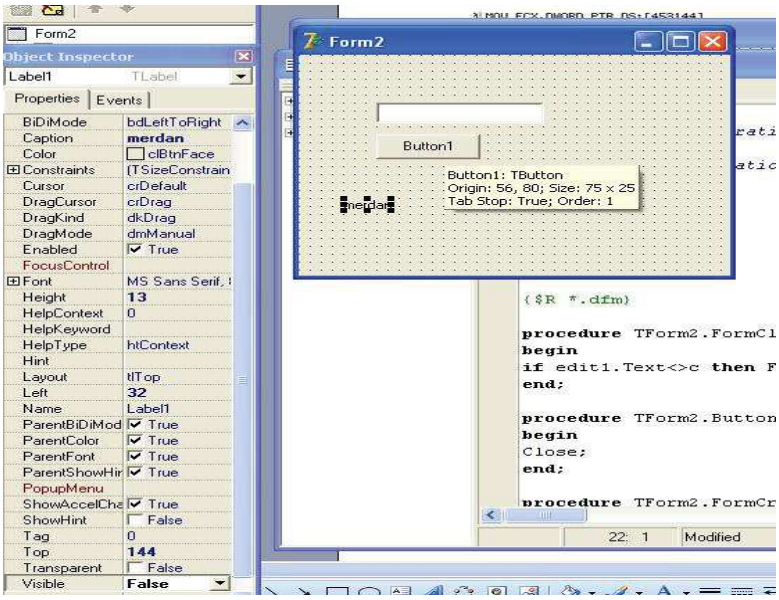

Рис 2 - Размещение пароля в свойствах компонента.

3. Дублирование критически важных данных в реестре

Для повышения устойчивости предлагается хранить копию паролей или контрольных строк в системном реестре.

Если злоумышленник попытается изменить данные в двоичном коде программы, они окажутся несоответствующими сведениям, записанным в реестре. В такой ситуации программа сможет обнаружить факт модификации, автоматически завершить свою работу, используя механизм самоуничтожения, и тем самым заблокировать попытку взлома [2].

4. Обнаружение запуска в дебаггере

Ключевым элементом функциональности является модуль DebaggerGarşy — специальная функция, которая позволяет определить, запущено ли приложение под отладчиком. В случае обнаружения такой попытки программа немедленно завершает работу и тем самым предотвращает доступ к своим внутренним данным [3].

Функция универсальна и не препятствует нормальной компиляции, но эффективно противодействует дизассемблированию .

Разработка выполнена как стандартное Windows-приложение на языке Delphi.

Система защиты работает следующим образом:

1. При запуске проверяется факт анализа через дебаггер (OllyDbg или любой другой отладчик).
2. Если анализ обнаружен, программа завершает выполнение.
3. Иначе продолжается нормальная работа.

Данный подход предназначен для применения в организациях, где важно обеспечить защиту программ от несанкционированного

доступа или внесения изменений. Представленная система безопасности может использоваться в коммерческом программном обеспечении, корпоративных приложениях, решениях, работающих с конфиденциальными данными, а также в случаях, когда требуется надёжная защита алгоритмов или бизнес-логики.

Методы защиты позволяют существенно осложнить анализ программы, повысить стоимость атаки и снизить вероятность успешного взлома.

В статье рассмотрены основные способы защиты Windows-приложений от анализа с использованием дебаггеров. На примере простой программы продемонстрированы характеристики уязвимости и предложены методы противодействия: скрытие строк, шифрование данных, хранение информации внутри машинного кода, дублирование в реестре и использование защитной функции DebaggerGarşy.

Такая многоуровневая защита позволяет значительно повысить устойчивость программы перед попытками взлома без ухудшения её работоспособности.

На данную разработку получено авторское свидетельство за №712 от 03.04.2025г., выданное Государственной службой Туркменистана по интеллектуальной собственности.

Список использованных источников

3. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие. - М.: ИД. "Форум": ИНФРА - М. 2013-592с.

4. Karl Maria Michael de Leeuw, Jan Bergstra - The History of Information Security: A Comprehensive Handbook, Elsevier Science, 2007.

5. M.Çuriýew. Maglumatlary goramak. Ýokary okuw mekdepleri üçin okuw kitaby. –A.: Türkmen döwlet neşirýat gullugy, 2013, 206 s.

УДК 004.9

Д.А. Бахытжан, Е.А. Спирина

Карагандинский национальный исследовательский университет имени академика Е.А. Букетова"

Караганда, Казахстан

РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ ПЕРСОНАЛИЗИРОВАННЫХ РЕКОМЕНДАЦИЙ В ТОРГОВЛЕ И КИНОИНДУСТРИИ НА ОСНОВЕ МАШИННОГО