защиты является наиболее надежным, так как может поддерживать строгую аутентификацию с использованием одноразовых паролей.

Все средства безопасности имеют свои недостатки, так и многофакторная аутентификация не является идеальной. Однако является более безопасной, чем традиционные механизмы защиты.

Список использованных источников

1. Герман Греф: я – игрок в долгую. 29 июня 2020 г. [Электронный ресурс]. – Режим доступа: https://tass.ru/business-officials/8827375 (дата обращения: 22.02.2023)

2. Чужиков, Н. О. Многофакторная аутентификация / Н. О. Чужиков. — Текст: непосредственный // Молодой ученый. — 2022. — № 21 (416). — С. 226-228. — URL: https://moluch.ru/archive/416/92149/ (дата обращения: 07.03.2023).

3. Статистика основных угроз безопасности в сетях ss7 мобильной связи. [Электронный ресурс] – URL: https://www.ptsecurity.com/upload/ptru/analytics/SS7-Vulnerability-2016-rus.pdf (дата обращения: 24.02.2023).

4. Галимов, Р.Р. Программно-аппаратные средства защиты информации в вычислительных системах: учебное пособие/ Р.Р. Галимов, А.А. Рычкова; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2017. – 132 с.

Чарикова Полина Вячеславовна, студент гр. 6271-110401D, charikova99@gmail.com.
Лофицкий Игорь Вадимович, к.т.н., доцент каф. радиотехники, ivl60@mail.ru.

УДК 004.056.5

РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ АППАРАТНОГО ТОКЕНА НА БАЗЕ СЕМЕЙСТВА МИКРОКОНТРОЛЛЕРОВ STM32

П.В. Чарикова, И.В. Лофицкий
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

Устройства, которые используются в системах безопасности, например, аппаратные токены, являются достаточно сложными системами, у которых развита внутренняя архитектура, и они имеют широкий спектр функций. Такие устройства должны отвечать жестким требованиям безопасности, так как от их корректной работы зависит правильность выполнения производственных процессов и т.д.

Главной составляющей таких устройств являются микроконтроллеры. Следовательно, микроконтроллеры становятся основной целью атаки злоумышленников. Основной проблематикой криптографической защиты на микроконтроллерах заключается в том, что, например, при использовании для защиты передачи данных секретный ключ, который хранится в памяти

микроконтроллера или даже в незащищённой отдельной микросхеме памяти, может быть считан с устройства при потере контроля над этим устройством.

Некоторые семейства микроконтроллеров уже включают множество функций безопасности. Примером может стать семейство микроконтроллеров STM32, у которого уже имеется множество встроенных функций, в том числе и обеспечивающих защиту [1].

Базовым механизмом безопасности является защита от чтения (RDP). Он предотвращает доступ к информации, которая содержится в памяти микроконтроллера, различными отладочными средствами. Это предотвращает сброс данных оперативной памяти. Защита кода позволяет ему только выполняться, но не записываться. В готовых серийных устройствах применение данного механизма рекомендуется во всех случаях.

Дополнительным средством защиты является блокировка отладки. Уровень безопасности можно выбрать в зависимости от требований, но потом изменить его уже будет нельзя. Прописываются определенные права, которые позволяют различным пользователям выполнять только определенные действия. Для этого встроенный модуль защиты памяти (MPU) разделяет память на области с различными правилами доступа и правами.

Функции защиты микроконтроллера также реализованы и на аппаратной основе в виде циклического контроля избыточного кода. Суть данного контроля заключается в вычислении контрольной суммы, которая помогает вычислять ошибки хранения и передачи данных.

Другими способами реализациями безопасности на аппаратной основе являются система безопасности тактирования (CSS) и мониторинг питания. Мониторинг питания позволяет обеспечивать сброс только с помощью аутентифицированного доступа, который осуществляется системой управления статусом, что наделяет данный метод высокой степенью защиты [2].

Главное содержимое USB-токена это генерируемый одноразовый пароль, который находится в памяти микроконтроллера. При несанкционированном доступе злоумышленник взламывает код, а также расшифровывает и зашифрованный пароль, и его алгоритм создания. Чтобы этого избежать используются определенные методы шифрования, в которых предусматриваются симметричные и ассиметричные методы шифрования. В некоторых серия STM32 для шифрования используется генератор случайных чисел. Процесс генерации случайных чисел основан на использовании источника шума. Набор из четырех 32-битных случайных чисел генерируется с максимальным периодом. Правилом генерации случайных чисел является следующее условие: чем ниже частота, тем выше энтропия.

Все эти перечисленные способы обеспечения криптозащиты присутствуют в различных сочетаниях в зависимости от конфигурации микроконтроллеров семейства STM32.

Список использованных источников
1. UM1924. User manual. STM32 crypto library. ST, 2015. [Электронный ресурс] – URL: https://www.st.com/resource/en/user_manual/dm00215061-stm32-crypto-library-stmicroelectronics.pdf (дата обращения: 26.10.2022).
2. Мартин Моц. Кибербезопасность на уровне микроконтроллеров. [Электронный ресурс] – URL: https://controleng.ru/wp-content/uploads/8370.pdf pdf (дата обращения: 26.10.2022).

Чарикова Полина Вячеславовна, студент гр. 6271-110401D, charikova99@gmail.com.
Лофицкий Игорь Вадимович, к.т.н., доцент каф. радиотехники, ivl60@mail.ru.

УДК 004.056.52; 004.891.3

ПОСТРОЕНИЕ DLP-СИСТЕМ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Е.А. Марченко, С.В. Жуков
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

Ключевые слова: DLP-системы, системы контроля, нейронные сети, нейросетевые технологии.

Предотвращение потери данных (Data Loss Prevention) - мера безопасности, предназначенная для защиты бизнес-информации и предотвращения потери, кражи и искажения важных или конфиденциальных данных путем предотвращения перемещения ключевой информации конечными пользователями за пределы сети. Технология использует программные или аппаратные инструменты, позволяющие сетевому администратору отслеживать данные, которые используются и передаются конечными пользователями.

DLP-система – программное решение либо набор инструментов, защищающая сетевые информационные структуры организации. Такая система позволяет анализировать данные защищаемого цифрового периметра безопасности на внешних носителях и т.п.

Искусственные нейронные сети (ИНС) обладают способностью к обучению, которое заключается в изменении весов и порогов сети. Самой распространённой из огромного множества различных вариаций ИНС является многослойная нейронная сеть прямого распространения (рисунок 1).

Сеть состоит из нескольких слоев и каждый из них состоит из искусственных нейронов, при этом выходы нейронов предыдущего слоя являются входами для нейронов последующего слоя. Она может моделировать функцию практически любой степени сложности, причем число слоев и число элементов в каждом слое определяют сложность функции.