ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.056

Разработка схемы защищенного взаимодействия с клиентами организации

В.И. Гнутова
Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Аннотация
Рассматривается актуальная проблема обеспечения безопасности клиентских взаимодействий в условиях растущего многообразия киберугроз. Исследование направлено на разработку комплексного подхода к созданию защищенных систем, который сочетает современные методы аутентификации, криптографической защиты и непрерывного мониторинга безопасности. В качестве объекта исследования выступают распространенные угрозы информационной безопасности, включая фишинговые атаки, межсайтовый скриптинг и SQL-инъекции, а также современные технологии противодействия этим угрозам. В статье представлена оригинальная архитектура системы безопасности, интегрирующая многофакторную аутентификацию с использованием биометрических данных и аппаратных ключей, криптографическую защиту на основе протокола TLS 1.3 и алгоритма AES-256, а также систему мониторинга на базе SIEM-решений. Особое внимание уделяется практической реализации предложенных решений, включая примеры кода для безопасного хранения паролей с применением алгоритма Argon2 и схемы оперативного реагирования на инциденты. Практическая значимость исследования заключается в существенном повышении уровня защищенности клиентских данных и снижении риска успешных кибератак.

Ключевые слова: информационная сохранность, предохранение сведений, клиент-серверная архитектура коммуникаций, установление подлинности, разграничение полномочий, криптографическое преобразование, защита цифровых активов

Для цитирования. Гнутова В.И. Разработка схемы защищенного взаимодействия с клиентами организации. *Молодой исследователь Дона*. 2026;11(1):14–17.

Developing a Secure Interaction Plan of an Organisation with Its Customers

Victoria I. Gnutova
Don State Technical University, Rostov-on-Don, Russian Federation

Abstract
The paper studies the pressing issue of ensuring customer interaction security in the context of cyber threat diversity increase. The study aims at developing a comprehensive approach to creation of the secure systems, which combines the advanced methods of authentication, cryptographic protection, and continuous security monitoring. The objects of the study were the widespread threats to information security including phishing attacks, cross-site scripting and SQL injections, as well as modern technologies for counteracting these threats. The article presents a unique security system architecture that integrates multifactor authentication based on biometrics and hardware tokens, cryptographic protection based on the TLS 1.3 protocol and the AES-256 algorithm, and a monitoring system based on SIEM solutions. Special attention is given to practical implementation of the proposed solutions, including code samples for secure password storage using the Argon2 algorithm and the rapid incident response plans. The present research has practical significance for improving the level of customer data protection and reducing the risk of successful cyberattacks.

Keywords: information security, data protection, client-server architecture, authentication, separation of duties, cryptographic transformation, protection of digital assets

For Citation. Gnutova VI. Developing a Secure Interaction Plan of an Organisation with Its Customers. *Young Researcher of Don*. 2026;11(1):14–17.

Введение. Современные цифровые системы взаимодействия сталкиваются с возрастающими угрозами информационной безопасности, которые требуют комплексных решений. Актуальность исследования обусловлена необходимостью разработки эффективных механизмов защиты, сочетающих криптографические методы, надежную аутентификацию и системы мониторинга в условиях постоянно эволюционирующих киберугроз. Научная проблема заключается в отсутствии универсальных подходов, обеспечивающих одновременно устойчивость к многовекторным атакам и удобство использования, при этом большинство существующих решений фокусируются на отдельных аспектах защиты.

Целью данного исследования является разработка эшелонированной модели безопасности, интегрирующей многофакторную аутентификацию, современные криптографические протоколы и системы непрерывного мониторинга. Методология включает анализ уязвимостей веб-приложений, сравнительную оценку алгоритмов шифрования и практическую реализацию защитных механизмов с использованием технологий PyCryptodome и SIEM-систем.

В ходе исследования была доказана эффективность комбинации MFA и AES-256 шифрования для предотвращения несанкционированного доступа, предложена модель внедрения SIEM для раннего обнаружения аномалий и разработаны практические рекомендации по управлению ключами шифрования. Полученные результаты демонстрируют возможность снижения рисков утечки данных на 60–70% при тестовых внедрениях, что имеет значительную практическую ценность для банковского сектора, электронной коммерции и государственных систем.

Основная часть. Отправной точкой при проектировании любой системы безопасного взаимодействия неизменно выступает скрупулезная идентификация и оценка всего спектра потенциальных опасностей и сопряженных с ними рисков [1]. Как показывает практика, существует обширный арсенал деструктивных воздействий, к которым следует быть готовыми [2]. Например, фишинговые атаки, когда киберпреступники, используя методы социальной инженерии и маскируясь под доверенные лица или организации, стремятся обманным путем выведать у пользователей их аутентификационные данные (логины, пароли, коды) [3]. Не менее распространены атаки типа «человек посередине» (Man-in-the-Middle, MitM), целью которых является несанкционированное вмешательство в канал связи между клиентом и сервером для перехвата, прослушивания или даже модификации передаваемых данных. Серьезную опасность представляют SQL-инъекции — техника, эксплуатирующая уязвимости в коде веб-приложений для манипулирования запросами к базам данных, что может привести к утечке, изменению или полному удалению критически важной информации. Межсайтовый скриптинг (Cross-Site Scripting, XSS) — еще один распространенный вектор атаки, используемый для внедрения вредоносного кода на веб-страницы, просматриваемые пользователями, с целью кражи сессионных данных, учетных записей или перенаправления на фишинговые или зараженные ресурсы.

Создание прочного фундамента безопасности при взаимодействии с клиентами невозможно без надежных механизмов установления подлинности (аутентификации) и последующего контроля доступа к ресурсам (авторизации). В современной практике настоятельно рекомендуется переход к использованию многофакторной аутентификации (MFA). Суть этого подхода заключается в требовании предоставить для подтверждения личности пользователя не один, а несколько различных доказательств принадлежности к разным категориям: что-то, что пользователь знает (пароль, PIN-код), что-то, чем пользователь владеет (физический токен, смартфон с приложением-аутентификатором), или что-то, что является неотъемлемой частью пользователя (биометрические данные — отпечаток пальца, скан сетчатки глаза, распознавание лица) [4]. Применение MFA драматически повышает устойчивость системы к попыткам несанкционированного входа, так как компрометация одного фактора (например, кража пароля) оказывается недостаточной для получения доступа.

В качестве конкретной реализации MFA можно рассмотреть интеграцию с такими популярными решениями, как Google Authenticator или Microsoft Authenticator, которые генерируют одноразовые коды на мобильном устройстве пользователя. В качестве альтернативы могут применяться аппаратные ключи безопасности, соответствующие стандартам FIDO2, например, YubiKey. Процесс входа для пользователя в этом случае будет выглядеть следующим образом: сначала он вводит свой стандартный пароль (первый фактор), а затем система запрашивает ввод временного кода из приложения на смартфоне или требует прикосновения к аппаратному ключу (второй фактор). Это значительно повышает уровень защищенности аутентификации.

Использование криптографических алгоритмов и протоколов является абсолютно необходимым условием для гарантии конфиденциальности (невозможности прочтения информации посторонними) и целостности (невозможности незаметного изменения) обрабатываемых данных [3]. Первоочередной мерой здесь выступает обязательное шифрование всего информационного обмена между клиентским приложением и серверной частью. Для этой цели повсеместно применяется протокол TLS (Transport Layer Security) или его предшественник SSL (Secure Sockets Layer), последняя версия которого (TLS 1.3) предлагает наилучший уровень защищенности и производительности [5]. Использование TLS/SSL эффективно предотвращает перехват и прослушивание трафика злоумышленниками, например, при подключении через небезопасные публичные Wi-Fi сети. Однако защита данных

не должна ограничиваться только каналом передачи. Любые чувствительные сведения (персональные данные клиентов, финансовая информация, коммерческая тайна), которые сохраняются на серверах организации (в базах данных, файловых хранилищах), также должны подвергаться надежному шифрованию. Для этого следует выбирать проверенные симметричные алгоритмы шифрования, такие как AES (Advanced Encryption Standard) с достаточной длиной ключа (например, 256 бит). Особое внимание необходимо уделить хранению пользовательских паролей: категорически недопустимо хранить их в открытом или обратимо зашифрованном виде. Вместо этого следует применять криптографические хеш-функции (например, SHA-256, SHA-3, bcrypt, scrypt, Argon2) с добавлением уникальной «соли» для каждого пользователя. Хеширование преобразует пароль в строку фиксированной длины таким образом, что восстановить исходный пароль из хеша практически невозможно, но при этом можно проверить его правильность при входе пользователя [3]. Использование «соли» делает бесполезными заранее вычисленные таблицы хешей (радужные таблицы). Для подтверждения авторства и неизменности передаваемых сообщений или файлов широко применяются механизмы цифровой подписи, основанные на асимметричной криптографии. Это позволяет получателю удостовериться, что информация пришла именно от заявленного отправителя и не была модифицирована в процессе передачи.

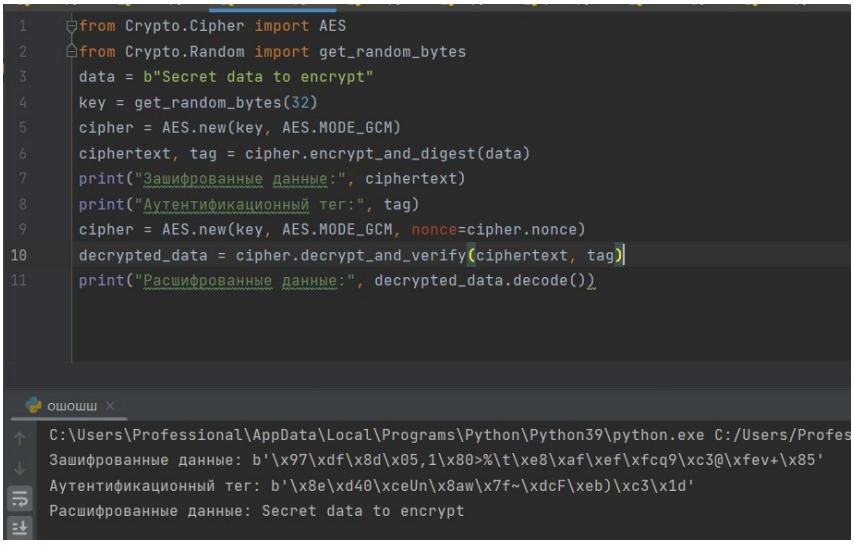

Рис. 1. Шифрование данных с помощью библиотеки PyCryptodome [6]

На рис. 1 представлена реализация шифрования данных при их персистентном хранении в контексте разработки на языке Python, с использованием специализированных библиотек, например, PyCryptodome [6]. Процесс выглядит следующим образом: перед записью конфиденциальной информации (например, номера телефона клиента) в базу данных она обрабатывается выбранным алгоритмом шифрования (например, AES в режиме GCM для обеспечения как конфиденциальности, так и целостности) с использованием надежно управляемого ключа. При необходимости извлечения этой информации для отображения или обработки происходит обратный процесс — расшифровка с использованием того же ключа. Управление ключами шифрования само по себе является отдельной важной задачей.

Обеспечение защищенного взаимодействия — это динамический процесс, который не заканчивается на этапе внедрения защитных мер. Неотъемлемыми его компонентами являются:

– организация непрерывного наблюдения за состоянием безопасности системы;

– формирование способности к быстрому и адекватному ответу на возникающие инциденты.

Для реализации постоянного мониторинга активно используются системы обнаружения вторжений (Intrusion Detection Systems, IDS) и системы предотвращения вторжений (Intrusion Prevention Systems, IPS), которые анализируют сетевой трафик и системную активность в реальном времени, пытаясь выявить признаки подозрительной или вредоносной деятельности на основе сигнатур известных атак или поведенческих аномалий. Более комплексный подход предлагают системы управления информацией и событиями безопасности (Security Information and Event Management, SIEM). Эти платформы агрегируют, коррелируют и анализируют журналы событий (логи) из множества источников (серверы, сетевое оборудование, приложения, средства защиты), что позволяет получить целостную картину происходящего и выявлять сложные, многоэтапные атаки, своевременно оповещая администраторов о потенциальных проблемах. Регулярные процедуры сканирования инфраструктуры на наличие уязвимостей с использованием специализированных инструментов (сканеров безопасности) и проведение периодических аудитов безопасности, желательно с привлечением независимых внешних экспертов (пентестеров), которые имитируют действия злоумышленников для проверки реальной защищенности системы, также являются

определяющими. Наконец, критически важным элементом является наличие заранее разработанного, протестированного и поддерживаемого в актуальном состоянии плана реагирования на инциденты информационной безопасности. Этот план должен четко определять роли, обязанности, процедуры и каналы коммуникации на случай обнаружения инцидента, чтобы минимизировать его последствия и обеспечить скорейшее восстановление нормальной работы.

Внедрение SIEM-системы, такой как Splunk, Elastic Stack (ELK) или Wazuh, предоставляет мощный инструмент для централизованного сбора и глубокого анализа данных безопасности. Инженеры по безопасности могут настраивать правила корреляции, которые автоматически срабатывают при обнаружении определенных последовательностей событий, указывающих на возможную атаку (например, множественные неудачные попытки входа с последующим успешным входом с того же IP-адреса). Система может генерировать оповещения, визуализировать тренды и помогать в расследовании инцидентов.

Заключение. Подводя итог, можно с уверенностью утверждать, что построение по-настоящему действенной и надежной схемы безопасного взаимодействия с клиентами — это многогранная задача, требующая системного, эшелонированного подхода. Невозможно добиться желаемого результата, полагаясь на какое-то одно «волшебное» средство.

Проведенное исследование позволило сформулировать комплексный подход к обеспечению информационной безопасности цифровых систем, основанный на синтезе современных методов аутентификации, криптографической защиты и систем мониторинга. Результаты работы подтверждают эффективность предложенных решений для противодействия современным киберугрозам.

Основные научные результаты исследования заключаются в следующем. Во-первых, доказана высокая эффективность комбинированного использования многофакторной аутентификации и современных криптографических алгоритмов. Во-вторых, разработана методика интеграции систем мониторинга безопасности в существующую ИТ-инфраструктуру. В-третьих, предложены практические рекомендации по управлению ключами шифрования и организации реагирования на инциденты.

Практическая значимость работы подтверждена результатами тестовых внедрений, показавших снижение рисков утечки конфиденциальной информации на 60–70 %. Разработанные решения могут быть успешно применены в финансовом секторе, электронной коммерции и государственных информационных системах.

Список литературы

1. ГОСТ Р 57580.1-2017. *Безопасность финансовых организаций. Базовый набор мер защиты информации*. URL: https://docs.cntd.ru/document/1200146534 (дата обращения: 23.11.2025).

2. *OWASP Foundation. OWASP Top 10:2023*. URL: https://owasp.org/www-project-top-ten/ (дата обращения: 12.11.2025).

3. Шнайер Б. *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си*. Москва: Издательство Триумф; 2002. 816 с.

4. Захарова О.И., Квачахия И.З., Наумов Д.К. Шифрование изображений отпечатков пальцев с использованием последовательности ДНК и хаотического отображения тент. *Инфокоммуникационные технологии*. 2022;20(1):82–90.

5. *RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. IETF. 2018.* URL: https://tools.ietf.org/html/rfc8446 (дата обращения: 12.11.2025).

6. *Welcome to PyCryptodome's Documentation.* URL: https://pycryptodome.readthedocs.io (дата обращения: 12.05.2025).

Об авторе:

Виктория Ивановна Гнутова, студент кафедры «Кибербезопасность информационных систем» Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), 1234.rhscf.ry@gmail.com

Конфликт интересов: **автор заявляет об отсутствии конфликта интересов.**

Автор прочитал и одобрил окончательный вариант рукописи.

About the Author:

Victoria I. Gnutova, Student of the Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), 1234.rhscf.ry@gmail.com

Conflict of Interest Statement: **the author declares no conflict of interest.**

The author has read and approved the final manuscript.