SATBAYEV UNIVERSITY

Computing & Engineering

Volume 1 (2023), Issue 2, 1-7

https://doi.org/10.51301/ce.2023.i2.01

Information security standards for Web-services

Ye. Aitkhozhayeva*, A. Muratkazhy

Satbayev University, Almaty, Kazakhstan

**Corresponding author: y.aitkhozhayeva@satbayev.university*

Abstract. Security problems and risks arising when using web services are inevitable due to the openness of the Internet. Traditional security mechanisms must be complemented by specific security structures. In solving this problem, it is necessary to focus on international standards, which contain the best techniques, practices and recommendations for ensuring the security of web services. The work reviewed three existing international standards and one internationally recognized US national standard in the field of information security. These standards address key aspects of standardization, such as security protocols, authentication methods, data encryption, and access control mechanisms. One of the fundamental standards in the field of information security, ISO/IEC 27001:2022, which sets criteria for information security management systems, is disclosed. The international standard ISO/IEC 27034, which consists of seven parts, is also considered. Each part of the standard focuses on a specific aspect of application information security. An analysis of the ISO 20078 standard, consisting of four parts, was carried out. This standard provides organizations and systems with a web services security model. The paper examines the US National Institute of Standards and Technology document 800-95 - the NIST SP 800-95 standard, which provides guidance on risk management, authentication, access control and encryption, adaptable to various types of web services. The issue of standardization of information security of web services by various international consortia and organizations is discussed. Generally recognized information security standards are the basis for organizing secure interaction for both the provider and the consumer of web services.

Keywords: *web-services, information security, international standards, national standards*.

1. Введение

Веб-сервисы стали ключевым элементом бизнес-процессов, обеспечивая удобство, доступность и эффективность взаимодействия между пользователями и информационными системами любого типа, в том числе обеспечивают взаимодействие систем B2B (бизнес-бизнес), B2C (бизнес-потребитель), C2C (потребитель-потребитель), B2G (бизнес-государство). Миллионы Веб-серверов образуют так называемую Всемирную Паутину. Веб-сервисы являются неотъемлемой частью современного цифрового мира и служат целям устойчивого развития (ЦУР) мирового сообщества. Но многие функции, которые делают Веб-сервисы привлекательными, включая большую доступность данных, идут вразрез с традиционными моделями безопасности и средствами контроля. В силу общедоступности сети Интернет, на основе которой функционируют Веб-сервисы, они привлекают большое количество злоумышленников. Обеспечение безопасности Веб-сервисов требует модификации традиционных механизмов безопасности, использование дополнительных структур безопасности, основанных на использовании механизмов аутентификации, авторизации, конфиденциальности и целостности. Защита Веб-приложений актуальна в любых условиях. В настоящее время предлагаются различные методы защиты Веб-приложений. Их выбор и реализация являются нетривиальной задачей. И здесь организациям и разработчикам Веб-сервисов надежную основу для выбора и реализации методов и механизмов в целях обеспечения целостности, конфиденциальности и доступности данных предоставляют соответствующие международные и национальные стандарты.

Стандарты информационной безопасности представляют собой набор лучших методов, практик, процедур, требований и тактик в области информационной безопасности. С их помощью обеспечиваются единые требования и методологии для управления рисками, для предотвращения и реагирования на кибератаки, для защиты информации и информационных услуг, в том числе предоставляемых Веб-сервисами.

Международные стандарты в области информационной безопасности разрабатываются Международной организацией по стандартизации - МОС (International Organization for Standardization - ISO), Международной электротехнической комиссией – МЭК (International Electrotechnical Commission - IEC), Международным союзом электросвязи (International Telecommunication Union - ITU). ITU был создан в 1865 году и является специализированным агентством Организации Объединенных Наций.

Несмотря на то, что национальный стандарт – это стандарт конкретного государства, но существуют национальные стандарты высокоразвитых стран, которые признаются мировым сообществом наравне с международными стандартами. Примером таких стандартов являются стандарты Национального института стандартов и технологий (NIST) США.

2. Материалы и методы

Ниже представлен анализ нескольких основных стандартов информационной безопасности, применимых для Веб-сервисов. Рассматриваются международные стандарты ISO/IEC 27001, ISO/IEC 27034, ISO 20078 и широко признанный национальный стандарт NIST.

Стандарт ISO/IEC 27001 - это международный стандарт, устанавливающий критерии создания, внедрения, обслуживания и постоянного улучшения системы управления информационной безопасностью (СУИБ или СМИБ) [1]. В основе стандарта лежат принципы, которые соответствуют бизнес-целям. Используется подход, основанный на оценке рисков и постоянном совершенствовании, охватывающий людей, процессы и технологии, с акцентом на конфиденциальность, целостность и доступность информации.

Структура стандарта ISO/IEC 27001 соответствует структуре Annex SL, общей для многих стандартов систем менеджмента ISO, что упрощает организациям интеграцию нескольких стандартов. К основным разделам стандарта относятся:

- область применения: определение границ СМИБ;
- нормативные ссылки: ссылки на другие стандарты, поддерживающие внедрение ISO/IEC 27001;
- термины и определения: разъяснение ключевых терминов, используемых в стандарте;
- контекст организации: понимание внутренних и внешних факторов, влияющих на управление информационной безопасностью организации;
- лидерство: установление приверженности лидерства и определение ролей и обязанностей;
- планирование: рассмотрение рисков и возможностей, а также определение целей СМИБ;
- поддержка: предоставление необходимых ресурсов, компетентности, осведомленности, коммуникации и документированной информации;
- эксплуатация: планирование и контроль процессов, необходимых для удовлетворения требований информационной безопасности;
- оценка эффективности: мониторинг, измерение, анализ и оценка СМИБ;
- улучшение: постоянное улучшение пригодности, адекватности и эффективности СМИБ.

Как было отмечено выше в основе ISO/IEC 27001 лежит подход, основанный на рисках. Организации обязаны выявлять и оценивать риски для информационной безопасности и внедрять средства контроля для управления и минимизации этих рисков. Процесс управления рисками включает оценку рисков, обработку рисков и регулярный анализ.

Организации часто стремятся получить сертификацию, чтобы доказать соответствие стандарту ISO/IEC 27001. Сертификация включает в себя аудит третьей стороной, обычно проводимый аккредитованными органами по сертификации. Получение сертификации означает, что СМИБ организации соответствует требованиям стандарта.

ISO/IEC 27001 подчеркивает важность постоянного улучшения. Организации должны регулярно пересматривать и совершенствовать свои методы обеспечения информационной безопасности учитывая внешние и внутренние изменения, а также результаты оценок производительности.

Внедрение ISO/IEC 27001 может принести организациям несколько преимуществ:

- защита конфиденциальной информации от несанкционированного доступа, раскрытия, изменения и уничтожения;
- помощь организациям в соблюдении соответствующих законов и правил, касающихся информационной безопасности;
- укрепление доверия с заинтересованными сторонами путем демонстрации приверженности информационной безопасности;
- получение конкурентного преимущества за счет удовлетворения ожиданий клиентов в отношении безопасной обработки информации;
- повышение эффективности за счет выявления и устранения рисков и уязвимостей.

ISO/IEC 27001 играет ключевую роль для компаний, стремящихся построить надежные системы управления информационной безопасностью. Направленность стандарта на оценку рисков и стремление к постоянному совершенствованию создают прочную основу для борьбы с постоянно развивающейся сферой угроз кибербезопасности.

Стандарт ISO/IEC 27034 ориентирован на применении мер безопасности внутри настроек безопасности приложений Этот стандарт предлагает подход к распознаванию, контролю и устранению угроз безопасности приложений на протяжении их жизненного цикла. ISO/IEC 27034 под общим названием Информационные технологии - Методы обеспечения безопасности - Безопасность приложений состоит из семи частей, каждая из которых посвящена определенным аспектам безопасности приложений.

В первой части (ISO/IEC 27034-1) выполняется обзор и излагаются основные концепции стандарта.

Целью второй части стандарта (ISO/IEC 27034-2) является содействие в создании, поддержке и проверке собственной нормативной структуры организации (НСО) в соответствии с требованиями, установленными в этом стандарте. Это необходимо для того, чтобы организации могли согласовывать или объединять свою НСО с корпоративной архитектурой организации и (или) системой менеджмента информационной безопасности.

Третья часть (ISO/IEC 27034-3) посвящена процессу управления безопасностью приложений. Дается система распознавания, контроля, уменьшения и устранения угроз безопасности на протяжении всего жизненного цикла приложения [2].

В четвертой части (ISO/IEC 27034-4) рассматриваются вопросы проверки и подтверждения безопасности приложения. Даются рекомендации, как систематически оценивать и гарантировать безопасность своих приложений, как подтвердить, что меры безопасности, реализуемые в приложениях, жизнеспособны и надежны. Это очень важно, так как приложения часто обрабатывают конфиденциальную информацию и выполняют базовые функции, что делает их привлекательными целями для киберугроз. Подчеркивая непрерывную проверку, тестирование и оценку как собственных, так и сторонних компонентов, стандарт способствует созданию безопасных, надежных и отказоустойчивых программных систем в постоянно развивающейся сфере кибербезопасности.

Пятая часть стандарта (ISO/IEC 27034-5) посвящена протоколам и структурам данных управления безопасностью приложений [3]. В этой части стандарта рассматриваются примеры распространенных опасностей и уязвимостей, возникающих в области безопасности приложений, предлагаются конкретные сценарии, подчеркивающие виды опасностей, с которыми могут столкнуться приложения. Все это помогает организациям понять эти проблемы и активно решать их. Основная цель ISO/IEC 27034-5 — предоставить организациям информацию для выявления потенциальных опасностей, с которыми приложения могут столкнуться на протяжении всего жизненного цикла.

Шестая часть (ISO/IEC 27034-6) представляет собой руководство по безопасности для конкретных приложений [4]. Посвящена анализу реальных примеров, является ценным ресурсом для организаций. В этих аналитических материалах описывается применение стандарта ISO/IEC 27034 в совершенно разных условиях. Также описывается, как организации эффективно реализуют меры безопасности в рамках жизненного цикла разработки своих приложений. На основе этого можно разработать свои собственные методологии для создания безопасных, надежных и успешных программных инфраструктур

В седьмой части (ISO/IEC 27034-7) рассматривается прогнозированное обеспечение безопасности приложений [5]. Эта часть фокусируется на аспектах администрирования безопасности приложений, даются рекомендации по созданию и поддержанию корректных структур администрирования, чтобы гарантировать организацию безопасности приложений. Также рассматриваются вопросы соответствия, подчеркивается важность обеспечения того, чтобы средства обеспечения безопасности приложений были адаптированы. Этот компонент администрирования гарантирует, что организации не только соответствуют законным требованиям, но и следуют лучшим в отрасли стандартам, развивая комплексный и надежный подход к безопасности приложений.

В заключение отметим, что ISO/IEC 27034 может стать комплексным стандартом, обеспечивающим всеобъемлющий и точный подход к безопасности приложений. Он представляет организациям мощную систему для включения безопасности в структуру форм разработки и организации приложений, что в конечном итоге повышает их гибкость против нарастающих киберугроз. Следование стандартам, изложенным в ISO/IEC 27034, позволяет организациям создавать и поддерживать безопасные приложения любого типа.

Стандарт ISO 20078 состоит из четырех частей и предлагает протокол связи для безопасного и надежного взаимодействия и совместной работы поставщика ресурсов и потребителя этих ресурсов через совместимые Веб-сервисы. Веб-сервисы были доступны на виртуальных машинах до создания этого стандарта, но не было стандартизации, особенно в отношении аутентификации и идентификации. Поэтому электронные транзакции не были достаточно защищены.

Стандарт ISO 20078-1 определяет все сущности и роли, используемые в серии ISO 20078. Стандарт определяет, как предлагающая сторона представляет ресурсы. В зависимости от категории ресурса поставщик использует разные виды идентификаторов. Такие ресурсы можно предоставлять напрямую или через контейнеры. Также описываются различные способы представления ресурсов в Веб-сервисах, таких как JSON и XML [6].

Стандарт ISO 20078-2 предлагает общий протокол связи, который обеспечивает доступ к ресурсам (URI): протокол передачи гипертекста (HTTP) поверх безопасности транспортного уровня (TLS), то есть HTTP-безопасность (HTTPS). Используя этот протокол, потребитель может безопасно получить доступ к ресурсам через Веб-службы предлагающей стороны [7].

Стандарт ISO 20078-3 предлагает стандартизированную модель безопасности Веб-сервисов. Используется ролевая модель, реализация которой совместима с протоколом авторизации OAuth 2.0 и аутентификации OpenID Connect. Модель включает различные роли и объекты, участвующие в политике авторизации. На предлагающей стороне три роли: поставщик удостоверений, поставщик авторизации и поставщик ресурсов. Дополнительные роли — это потребитель ресурса и владелец ресурса, который отвечает за свои ресурсы [8].

Стандарт ISO 20078-4 представляет логические процессы взаимодействия всех выше определенных ролей и объектов. Процессы, связанные с регистрацией, аутентификацией и авторизацией стороны-потребителя, удовлетворяют требованиям, представленным в предыдущих частях стандарта. В описываемых процессах полнлстью отражено взаимодействие между участниками системы: регистрация между объектами, предоставление и отзыв доступа, возможность управления контейнерами и т.д. [9].

Следование стандарту ISO 20078 обеспечивает развитие взаимодействующих и надежных электронных систем с электронными транзакциями через безопасное предоставление доступа, отказ, отзыв и управление контейнерами.

Стандарт NIST SP 800-95 (Security and Privacy Controls for Information Systems and Organizations) [10]. Специальная публикация 800-95 Национального института стандартов и технологий (NIST), озаглавленная «Руководство по обеспечению безопасности Веб-сервисов», входящая в серию NIST SP 800, играет ключевую роль в формировании стратегий защиты цифровых активов и конфиденциальной информации.

NIST SP 800-95 предоставляет адаптируемые к различным типам Веб-сервисов рекомендации по внедрению эффективных средств контроля безопасности и конфиденциальности для Веб-сервисов, рассматривая управление рисками, аутентификацию, контроль доступа и шифрование. В документе изложен набор требований по обеспечению безопасности Веб-порталов, затрагивающий различные аспекты аутентификации, авторизации и защиты данных, исходя из схемы взаимодействия пользователя, Веб-портала, поставщика идентификационной информации и поставщика Веб-служб, представленной на рисунке 1.

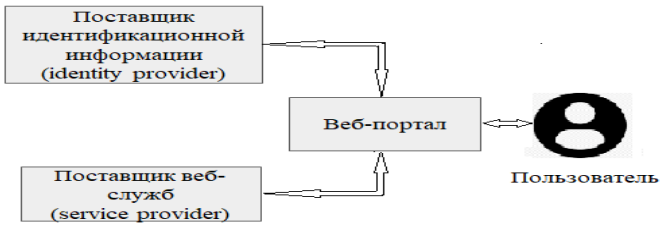

Рисунок 1. Схема взаимодействия пользователя, Веб-портала, поставщика идентификационной информации и поставщика Веб-служб

Схема взаимодействия пользователя, Веб-портала, поставщика идентификационной информации и поставщика Веб-служб помогает понять процессы аутентификации, авторизации и предоставления услуг пользователей в среде Веб-систем.

Веб-портал служит точкой входа пользователя, заинтересованного в безопасности своих данных, в сервис-ориентированную архитектуру (SOA). Это своего рода шлюз, через который пользователь может получить различные сервисы. Поставщики, встроенные в сервис-ориентированную архитектуру, предлагают свои ресурсы с учетом обеспечения их защищенности.

Пользователь инициирует доступ к защищенным ресурсам Веб-портала, а Веб-портал запрашивает аутентификацию у поставщика удостоверений, так как именно поставщик удостоверений ответственен за проверку учетных данных пользователя. По результату проверки поставщик удостоверений отвечает сообщениями на языке разметки утверждений безопасности SAML (Security Assertion Markup Language) — криптографическим подтверждением аутентификации пользователя. Эти утверждения служат мандатами доверия, предоставляя которые пользователь может легально взаимодействовать с поставщиками Веб-сервисов.

Проверив сообщения SAML, поставщик Веб-услуг получает информацию, подтверждающую как легальность и подлинность пользователя, так и подтверждение его прав на выполнение запрошенных действий. Это один из основных моментов процесса, который служит для предотвращения несанкционированного доступа к конфиденциальной информации. Получив SAML, поставщик открывает доступ к своим защищенным Веб-сервисам (услугам, функциям, приложениям, службам).

Предлагаемая стандартом NIST 800-95 схема предоставления услуг пользователей в среде Веб-систем обеспечивает поддержание безопасной среды и предотвращает несанкционированный доступ к конфиденциальной информации.

Рисунок 2. Базовые требования стандарта NIST SP 800-95

Публикация NIST 800-95 (NIST SP 800-95) содержит полный набор требований, направленных на обеспечение безопасности Веб-порталов. Эти требования охватывают различные аспекты аутентификации, авторизации, защиты данных, аудита и документирования. Для наглядности, базовые требования стандарта NIST SP 800-95 к обеспечению безопасности Веб-порталов представлены на рисунке 2.

Ниже представлены базовые требования стандарта NIST SP 800-95 с указанием их направленности на обеспечение конкретных аспектов информационной безопасности.

Аутентификация: требуется использование методов многофакторной аутентификации для пользователей веб-порталов. Многофакторная аутентификация более надежная, так как при этом используется несколько факторов подтверждения подлинности пользователя: пароли, смарт-карты, токены или биометрические данные.

Авторизация: для понижения риска несанкционированного доступа рекомендуется применение дискреционного контроля доступа с использованием привилегий, выданных пользователям через тщательно определенные их роли.

Аудит: необходимо организовать учет доступа пользователей к веб-порталам, используя механизмы мониторинга и аудита для обеспечения подотчетности и обнаружения несанкционированного доступа.

Целостность (непротиворечивость): рекомендуется использовать шифрование и хеширование для обеспечения такой характеристики информационной безопасности, как целостность. Это необходимо, чтобы предотвратить неправомочное изменение информации, хранящейся на веб-порталах. Подчеркивается необходимость методов безопасного кодирования Веб-приложений для предотвращения уязвимостей. А также необходимо внедрять средства постоянного контроля за обеспечением целостности Веб-сервисов.

Конфиденциальность: необходимо на веб-портале иметь политику конфиденциальности, определяющую меры по защите конфиденциальных пользовательских данных. Эта политика безопасности должна быть известной, основана на правилах и стандартах информационной безопасности, включать не только меры по защите данных, но и средства контроля конфиденциальности, чтобы гарантировать поддержку конфиденциальности.

Приватность (коррелируется с конфиденциальностью): рекомендуется иметь, периодически обновляемую с учетом законодательства, политику приватности для веб-порталов, то есть все пользователи должны иметь информацию, как их данные будут собираться, использоваться и защищаться. Требуется использовать механизмы шифрования для защиты, в том числе и при передаче, критических данных пользователя. Необходимо для конфиденциальности использовать безопасные протоколы связи, такие как HTTPS.

Доступность (является важной характеристикой информационной безопасности): веб-портал должен быть доступен всегда для легальных пользователей, и эта доступность должна оцениваться. Для обеспечения этой возможности необходимо иметь реализованные решения по резервированию и аварийному переключению, подлежащие периодическому тестированию в целях устранения потенциальных уязвимостей. Это обеспечит защиту от сбоев системы. Так как бизнес требует непрерывности процесса, то обязательно наличие плана обеспечения непрерывности бизнеса и аварийного восстановления для поддержания функциональности портала.

Неподдельность (коррелируется с целостностью): требуется постоянная проверка целостности для выявления и реагирования на неправомерные изменения данных. Необходимо иметь надежные механизмы валидации данных, что обеспечит адекватность информации, использовать безопасное кодирование для смягчения уязвимостей, которые могут подвергнуть опасности целостность данных. Регулярно выполнять анализ безопасности

кода для выявления и устранения потенциальных уязвимостей.

Администрирование политик (коррелируется с конфиденциальностью и приватностью): наличие регулярно обновляемых комплексных политик безопасности, регулирующих администрирование веб-портала, в которых должны быть определены роли и обязанности, связанные с администрированием политик. Угрозы, направленные на Веб-сервисы, постоянно развиваются, развиваются и средства защиты, в связи с чем политики безопасности должны регулярно пересматриваться.

Стандарт NIST SP 800-95 представляет собой ценное руководство в области информационной безопасности по защите цифровых активов и конфиденциальной информации.

Представленные выше стандарты информационной безопасности играют важную роль в формировании единого подхода к безопасности и стандартизации в использовании Веб-сервисов. Эти стандарты предоставляют обширные рекомендации, тактики, техники, процедуры и требования, приняв которые организации могут защитить свои Веб-сервисы от множества киберугроз, обеспечивая безопасную и отказоустойчивую цифровую инфраструктуру.

3. Результаты и обсуждение

Технологическое и социологическое направление развития Всемирной Паутины определяет Консорциум World Wide Web Consortium (W3C), в рамках которого постоянно ведется работа по разработке стандартов информационной безопасности Веб-сервисов. Существуют международные организации и рабочие группы, целью которых является разработка, развитие и продвижение различных стандартов в сфере информационной безопасности, в том числе и безопасности Веб-сервисов, с ориентиром на международные стандарты. Лидирующей организацией по разработанным стандартам, относящихся к Веб-сервисам, является консорциум OASIS (Organization for the Advancement of Structured Information Standards). В его работе задействовано более 5000 специалистов из более чем 600 организаций из 100 стран мира. Деятельность консорциума спонсируется такими корпорациями, как IBM, Novell, Oracle, Microsoft. OASIS - это организация по совершенствованию стандартов структурированной информации. Его Технические комитеты разрабатывают спецификации и стандарты. Язык разметки утверждений безопасности SAML на основе языка XML для обмена данными аутентификации и авторизации при взаимодействии поставщика и потребителя Веб-услуги (использован в стандарте NIST SP 800-95) был разработан именно в OASIS. В его состав входит Технический комитет OASIS Web Services Security (WSS) и организация OASIS Web Services Interoperability, которые специализируются на стандартизации информационной безопасности Веб-сервисов [11, 12].

Среди стандартов и спецификаций информационной безопасности Веб-сервисов, основными, согласно NIST Guide to Secure Web Services, являются стандарты и спецификации, представленные на рисунке 3 [13]. Наиболее интересные из них раскрыты ниже.

WebTrust (WS-Trust) представляет собой программу аттестации и сертификации, которая была разработана Американским институтом дипломированных общественных бухгалтеров AICPA ((American Institute of Certified Public Accountants) и Канадским институтом учетных данных CICA (Canadian Institute of Chartered Accountants). Эта программа содержит стандарты и критерии для аудиторской оценки и подтверждения безопасности, конфиденциальности, целостности и доступности электронных коммерческих транзакций и информационных систем в Интернете.

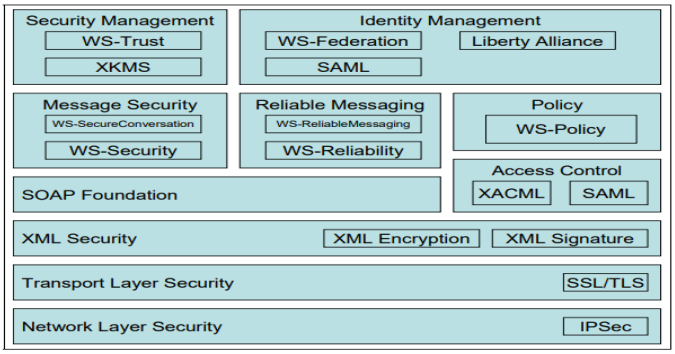

Рисунок 3. Основные стандарты и спецификации информационной безопасности Веб-сервисов

Организации, предоставляющие услуги в Интернете с использованием Веб-технологии, могут подтвердить конфиденциальность и надежность своих процессов электронной коммерции, пройдя аудит в соответствии с требованиями WebTrust. Программа охватывает различные аспекты, включая защиту данных, конфиденциальность пользователя, безопасность транзакций и обеспечение доступности сервисов. В WebTrust имеются также требования, касающиеся защиты персональных данных в онлайновой среде, в которой персональная информация, полученная в результате интернет-операций, собирается, используется, раскрывается и хранится согласно договору.

Стандарт WS-Security описывает процессы аутентификации и авторизации в среде обмена SOAP (Simple Object Access Protocol) сообщениями. Протокол SOAP появился еще в 1998 году (благодаря спонсированию корпорации Microsoft) и был передан международному консорциуму World Wide Web Consortium (W3C), который разрабатывает и внедряет технологические рекомендации для Всемирной паутины.

WS-Security предусматривает аутентификацию пользователя с использованием идентификации и аутентификации (логин и пароль), сертификатов X.509 или протокола Kerberos. Эти же технологии реализуют цифровую подпись, которая используется для подтверждения истинности (целостности) сообщения. В стандарте WS-Security также определены механизмы шифрования SOAP-сообщений путем использования стандарта XML Encryption.

WS-Reability представляет собой спецификацию для гарантированной и надежной доставки и упорядочения сообщений Веб-сервисов, а также удаления дубликатов сообщений. Можно сказать, что это модификация и расширение протокола SOAP, что обеспечивает независимость от платформы и производителя, нет привязки к базовому транспортному протоколу. В разработке WS-Reability приняли участие такие мировые IT корпорации,

как Fujitsu, Hitachi, NEC, Oracle, Sonic Software и Sun Microsystems.

WS-Policy - это спецификация, которая используется для описания разнообразия политик Web-сервисов. Определяется универсальная инфраструктура, которая может быть расширена другими спецификациями Web-сервисов, определяет политику как набор одного или более утверждений политики.

WS-Federation - это расширение WS-Trust, основанное на спецификациях WS-Security и WS-Policy.

4. Выводы

Веб-сервисы обеспечивают доступность и интегрируемость разнородных приложений, используя общедоступную сеть Интернет. Они не ограничены периметром сети, данные передаются в формате XML, пропускаемом многими межсетевыми экранами. Все эти особенности предоставляют злоумышленникам широкие возможности для кибератак.

Согласно мнению аналитиков организации OASIS Web Services Interoperability, главные угрозы, нацеленные на Web-сервисы: несанкционированные изменения сообщений, потеря их конфиденциальности и аутентичности отправителей, DoS-атаки.

И в этом мире угроз и уязвимостей стандарты служат ценным ресурсом для инженеров, экспертов по безопасности и лиц, принимающих решения, являются основой для реализации эффективных мер безопасности Веб-сервисов. Международные стандарты обновляются с периодичностью три, пять или семь лет с учетом новых киберугроз и рисков, с адаптацией к изменяющимся условиям информационной безопасности.

Стандарты информационной безопасности Веб-сервисов устанавливают общепринятые нормы, правила, требования и рекомендации для защиты Веб-сервисов относительно аутентификации и авторизации, шифрования данных, защиты от кибератак, управления уязвимостями. А также, что очень важно, помогают соответствовать различным регуляторным и правовым требованиям в конкретном регионе или государстве, например, таким как GDPR (General Data Protection Regulation) в странах Европейского союза, HIPAA (Health Insurance Portability and Accountability Act) в США, PCI DSS (Payment Card Industry Data Security Standard) во всем мире, так как это международный стандарт безопасности данных платежных карт и транзакций.

References / Литература

[1] ISO/IEC 27001:2022(en). Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO Online Browsing Platform. *Retrieved from:* https://www.iso.org/ru/standard/27001

[2] ISO/IEC 27034-3:2018(en). Information technology — Application security — Part 3: Application security management process. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/ru/standard/55583.html

[3] ISO/IEC 27034-5:2017(en). Information technology — Security techniques — Application security. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/standard/55585.html

[4] ISO/IEC 27034-6:2016(en). Information technology — Security techniques — Application security. ISO Online Browsing Platform *Retrieved from*: https://www.iso.org/standard/60804.html

[5] ISO/IEC 27034-7:2018 (en). Information technology — Application security— Part 7: Assurance prediction framework. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/standard/66229.html

[6] ISO 20078-1:2021 (en). Road vehicles — Extended vehicle (ExVe) web services — Part 1: Content and definitions. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/standard/80183.html

[7] ISO 20078-2:2021 (en). Road vehicles - Extended vehicle (ExVe) web services — Part 2: Access. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/standard/80184.html

[8] ISO 20078-3:2021 (en). Road vehicles — Extended vehicle (ExVe) web services — Part 2: Access. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/ru/standard/80185.html

[9] ISO/TR 20078-4:2021 (en). Road vehicles — Extended vehicle (ExVe) web services — Part 4: Control. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/standard/80186.html

[10] NIST SP 800-95 (en). Information Technology Laboratory — Computer Security Resource Center- Guide to Secure Web Services. NIST Computer Security Resource Center. *Retrieved from*: https://csrc.nist.gov/pubs/sp/800/95/final

[11] OASIS Web Services Security (WSS) TC (en). *Retrieved from*: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

[12] OASIS Web Services-Interoperability (WS-I). Member Section (en). *Retrieved from*: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ws-i-ms

[13] NIST SP 800-95. Guide to Secure Web Services. Recommendations of the National Institute of Standards and Technology (en). *Retrieved from*: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-95.pdf

Web-қызметтердің ақпараттық қауіпсіздік стандарттары

Е. Айтқожаева*, А. Мұратқажы

Satbayev University, Алматы, Қазақстан

**Корреспонденция үшін автор: y.aitkhozhayeva@satbayev.university*

Аңдатпа. Интернеттің ашықтығына байланысты Веб-қызметтерді пайдалану кезінде туындайтын қауіпсіздік мәселелері мен тәуекелдер болуы сөзсіз. Дәстүрлі қауіпсіздік тетіктері арнайы қауіпсіздік құрылымдарымен толықтырылуы керек. Бұл мәселені шешуде Веб-қызметтердің қауіпсіздігін қамтамасыз ету бойынша озық әдістерді, тәжірибелерді және ұсыныстарды қамтитын халықаралық стандарттарға назар аудару қажет. Жұмыста ақпараттық қауіпсіздік саласындағы үш қолданыстағы халықаралық стандарт пен бір халықаралық мойындалған АҚШ ұлттық стандарты қарастырылды. Бұл стандарттар қауіпсіздік хаттамалары, аутентификация әдістері, деректерді шифрлау

және қол жеткізуді басқару механизмдері сияқты стандарттаудың негізгі аспектілерін қарастырады. Ақпараттық қауіпсіздікті басқару жүйесінің критерийлерін белгілейтін ақпараттық қауіпсіздік саласындағы іргелі стандарттардың бірі ISO/IEC 27001:2022 қарастырылды. Жеті бөліктен тұратын ISO/IEC 27034 халықаралық стандарты да қарастырылған. Стандарттың әрбір бөлігі қолданбалы ақпаратты қорғаудың белгілі бір аспектісіне бағытталған. Төрт бөліктен тұратын ISO 20078 стандартының талдауы жүргізілді. Бұл стандарт ұйымдар мен жүйелерді Веб-қызметтердің қауіпсіздік үлгісімен қамтамасыз етеді. Ғылыми жұмыста АҚШ Ұлттық стандарттар және технологиялар институтының 800-95 құжаты – NIST SP 800-95 стандарты қарастырылды, ол тәуекелдерді басқару, аутентификация, қол жеткізуді бақылау және шифрлау бойынша нұсқауларды береді, Веб-қызметтердің әртүрлі түрлеріне бейімделеді. Әртүрлі халықаралық консорциумдар мен ұйымдардың Веб-қызметтердің ақпараттық қауіпсіздігін стандарттау мәселесі талқыланды. Ақпараттық қауіпсіздіктің жалпы танылған стандарттары Веб-қызметтерді жеткізуші үшін де, тұтынушы үшін де қауіпсіз өзара әрекеттесуді ұйымдастырудың негізі болып табылады.

Негізгі сөздер: *веб-қызметтері, ақпараттық қауіпсіздік, халықаралық стандарттар, ұлттық стандарттар*.

Стандарты информационной безопасности web-сервисов

Е. Айтқожаева*, А. Мұратқажы

Satbayev University, Алматы, Казахстан

**Автор для корреспонденции: y.aitkhozhayeva@satbayev.university*

Аннотация. Проблемы безопасности, риски, возникающие при использовании Веб-сервисов неизбежны в связи с открытостью Интернет сети. Традиционные механизмы безопасности должны быть дополнены специфическими структурами безопасности. В решении этой проблемы необходимо ориентироваться на международные стандарты, в которых собраны лучшие техники, практики и рекомендации по обеспечению безопасности Веб-сервисов. В работе выполнен обзор трех существующих международных стандартов и одного, признанного мировым сообществом, национального стандарта США в области информационной безопасности. В этих стандартах рассмотрены ключевые аспекты стандартизации, такие как протоколы безопасности, методы аутентификации, шифрование данных и механизмы контроля доступа. Раскрыт один из основополагающих в области информационной безопасности стандарт ISO/IEC 27001:2022, который устанавливает критерии для систем управления информационной безопасностью. Рассматривается также международный стандарт ISO/IEC 27034, который состоит из семи частей. Каждая часть стандарта посвящена определенному аспекту информационной безопасности приложений. Выполнен анализ стандарта ISO 20078, состоящего из четырех частей. Данный стандарт предлагает организациям и системам модель безопасности Веб-сервисов. В работе рассматривается документ 800-95 Национального института стандартов и технологий США - стандарт NIST SP 800-95, который представляет собой руководство по управлению рисками, аутентификации, контроля доступа и шифрования, адаптируемое к различным типам Веб-сервисов. Обсуждается вопрос стандартизации информационной безопасности Веб-сервисов различными международными консорциумами и организациями. Общепризнанные стандарты информационной безопасности являются основой для организации безопасного взаимодействия как для поставщика, так и для потребителя Веб-сервисов.

Ключевые слова: *веб-сервисы, информационная безопасность, международные стандарты, национальные стандарты*.

Received: 05 March 2023
Accepted: 15 June 2023
Available online: 30 June 2023