УНИФИКАЦИЯ СТАНДАРТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЕДИНЫЙ ПОДХОД К ПОВЫШЕНИЮ КИБЕРУСТОЙЧИВОСТИ ОРГАНИЗАЦИЙ

Серикказин Аян Есейулы

магистрант, Евразийский Национальный Университет им Л. Н. Гумилева – ЕНУ, Казахстан, г. Астана

Нурушева Асель Муратовна

PhD, и.о. доцента кафедры Информационная безопасность, Евразийский Национальный Университет им Л. Н. Гумилева – ЕНУ, Казахстан, г. Астана

UNIFICATION OF INFORMATION SECURITY STANDARDS: A UNIFIED APPROACH TO ENHANCING ORGANIZATIONS' CYBER RESILIENCE

Ayan Serikkazin

Undergraduate, L.N. Gumilyov Eurasian National University - ENU, Kazakhstan, Astana

Assel Nurusheva

PhD, acting associate professor of the department of Information Security, Eurasian National L.N. Gumilyov Eurasian National University - ENU, Kazakhstan, Astana

Аннотация. В данной статье рассматривается гармонизация стандартов информационной безопасности, таких как ISO/IEC 27001, NIST SP 800-53 и CIS Critical Security Controls, для повышения киберустойчивости организаций. Анализируя сходства и различия между этими стандартами, в исследовании предлагается создание единой система, которая включает в себя их сильные стороны. Полученная система предлагает комплексный подход к кибербезопасности, способствующий повышению эффективности, сокращению дублирования усилий и более тесному согласованию с целями организации.

Abstract. This article explores the harmonization of information security standards, such as ISO/IEC 27001, NIST SP 800-53, and CIS Critical Security Controls, to improve organizations' cyber resilience. By analyzing similarities and differences between these standards, the study proposes a unified framework that incorporates their respective strengths. The resulting framework offers a comprehensive approach to cybersecurity, promoting efficiency, reduced duplication of efforts, and increased alignment with organizational goals.

Ключевые слова: стандарты информационной безопасности; единый подход; постоянное совершенствование; лучшие практики; информационная безопасность; управление рисками.

Keywords: information security standards; unified approach; continuous improvement; best practices; information security; risk management.

Введение. Быстрый прогресс технологий и растущая зависимость от цифровых систем подвергают организации огромному количеству киберугроз. Эти угрозы могут привести к серьезному финансовому и репутационному ущербу, что делает необходимым для организаций принятие эффективных мер информационной безопасности. Для решения этой задачи были разработаны различные стандарты и системы информационной безопасности, которые содержат рекомендации для организаций по внедрению и поддержанию надежных средств контроля безопасности.

Однако организации часто сталкиваются с проблемами при выборе и внедрении наиболее подходящего стандарта или системы, поскольку каждый из них имеет свою уникальную направленность, сферу применения и требования. В данной статье предлагается согласованный подход к стандартам информационной безопасности, объединяющий ключевые принципы и лучшие практики ISO/IEC 27001, NIST SP 800-53 и CIS Critical Security Controls в единую структуру, которая может быть адаптирована к различным организационным условиям.

Обзор литературы

1. ISO/IEC 27001:2013 – это международный стандарт, разработанный Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC), обеспечивающий основу для создания, внедрения, поддержания и постоянного улучшения системы менеджмента информационной безопасности (ISMS) [1]. Стандарт основан на модели Plan-Do-Check-Act (PDCA) и охватывает людей, процессы и технологии. ISO/IEC 27001:2013 делает акцент на управлении рисками, требуя от организаций выявлять, оценивать и обрабатывать риски, связанные с их информационными активами, для достижения приемлемого уровня риска.

2. NIST SP 800-53 – это стандарт, разработанный Национальным институтом стандартов и технологий (NIST) и содержащий рекомендации для федеральных агентств и их подрядчиков по защите их информационных систем и организаций от рисков безопасности [2]. Стандарт ориентирован на выбор и внедрение средств контроля безопасности на основе допустимого риска организации и категоризации ее информационных систем. NIST SP 800-53 состоит из 18 семейств средств контроля, включающих более 900 средств контроля, относящихся к различным технологиям и системам.

3. CIS Critical Security Controls – это набор приоритетных действий для улучшения информационной безопасности, разработанный глобальным сообществом экспертов по кибербезопасности [3]. Эти элементы управления призваны помочь организациям выявить и смягчить наиболее распространенные и критические уязвимости безопасности. CSC состоит из 20 элементов контроля, охватывающих различные аспекты информационной безопасности, такие как управление активами, контроль доступа и реагирование на инциденты. Элементы контроля имеют приоритеты, предоставляя организациям "дорожную карту" для постепенного повышения уровня безопасности путем систематического внедрения элементов контроля.

Общие черты и различия. Обзор литературы выявил несколько общих черт и различий между ISO/IEC 27001:2013, NIST SP 800-53 и CIS Critical Security Controls. Некоторые из ключевых сходств включают их фокус на управлении рисками, принятие многоуровневого подхода к безопасности и акцент на постоянном совершенствовании. Тем не менее, они различаются по сфере применения, целевой аудитории и степени детализации элементов управления безопасностью.

1. Управление рисками: Все три стандарта подчеркивают важность управления рисками для достижения эффективной информационной безопасности. ISO/IEC 27001:2013 требует от организаций проводить регулярные оценки рисков и внедрять соответствующие меры по

управлению рисками, а NIST SP 800-53 и CIS Critical Security Controls сосредоточены на выборе и внедрении средств контроля безопасности на основе профиля рисков организации и критичности ее информационных систем. Интегрированная методология оценки рисков, объединяющая основанный на оценке рисков подход ISO/IEC 27001 и NIST Cybersecurity Framework, может помочь организациям определить приоритетность средств контроля безопасности и ресурсов на основе конкретной среды рисков [4]

2. Многоуровневый подход к безопасности: Стандарты признают необходимость многоуровневого подхода к безопасности, рассматривая различные аспекты информационной безопасности, такие как физический, технический и административный контроль. Такой подход обеспечивает наличие нескольких уровней защиты, снижая вероятность успешной кибератаки.

3. Непрерывное совершенствование: Стандарты подчеркивают важность постоянного совершенствования для поддержания эффективной системы безопасности. ISO/IEC 27001:2013 следует модели PDCA, требуя от организаций регулярного пересмотра и совершенствования своей СУИБ, а NIST SP 800-53 и CIS Critical Security Controls выступают за постоянный мониторинг и оценку средств контроля безопасности для выявления и устранения любых пробелов или слабых мест.

4. Сфера применения: ISO/IEC 27001:2013 имеет более широкую сферу применения, охватывая общее управление информационной безопасностью и будучи применимым к организациям любого размера, типа или отрасли. NIST SP 800-53 в первую очередь ориентирован на федеральные агентства США и их подрядчиков, хотя он может использоваться в качестве справочника и другими организациями. CIS Critical Security Controls нацелен на наиболее распространенные и критические уязвимости безопасности, предлагая приоритетный подход к информационной безопасности.

5. Целевая аудитория: ISO/IEC 27001:2013 предназначен для организаций любого размера, типа или отрасли, в то время как NIST SP 800-53 разработан в первую очередь для федеральных агентств США и их подрядчиков. CIS Critical Security Controls применим для более широкой аудитории, включая организации частного сектора и некоммерческие организации.

6. Гранулярность контроля безопасности: NIST SP 800-53 предоставляет более детальный набор средств контроля безопасности по сравнению с ISO/IEC 27001:2013 и CIS Critical Security Controls. NIST SP 800-53, содержащий более 900 элементов контроля, объединенных в 18 семейств элементов контроля, предлагает комплексный и детальный подход к информационной безопасности. В отличие от него, ISO/IEC 27001:2013 включает 114 элементов контроля, разделенных на 14 категорий, а CIS Critical Security Controls состоит из 20 приоритетных элементов контроля.

Согласование стандартов информационной безопасности. Учитывая общие черты и различия между стандартами, единый подход к стандартам информационной безопасности может быть разработан путем интеграции ключевых принципов и лучших практик из ISO/IEC 27001:2013, NIST SP 800-53 и CIS Critical Security Controls. Этот согласованный подход должен включать в себя следующие элементы:

1. Подход, основанный на оценке рисков: Принять подход к информационной безопасности, основанный на оценке рисков, обеспечивающий выбор и внедрение средств контроля безопасности на основе профиля рисков организации и критичности ее информационных систем.

2. Многоуровневая безопасность: Применяйте многоуровневый подход к безопасности, который затрагивает различные аспекты информационной безопасности, включая физические, технические и административные средства контроля.

3. Непрерывное совершенствование: Подчеркивать важность постоянного совершенствования для поддержания эффективной системы безопасности, требуя от организаций регулярно анализировать, оценивать и совершенствовать свои средства и методы контроля безопасности.

4. Масштабируемость и гибкость: Убедитесь, что гармонизированная структура является масштабируемой и гибкой, позволяя организациям различных размеров, типов и отраслей адаптировать структуру к своим конкретным потребностям и требованиям.

5. Интеграция лучших практик: Использовать лучшие практики и ключевые принципы из ISO/IEC 27001:2013, NIST SP 800-53 и CIS Critical Security Controls, создавая всеобъемлющий и целостный набор средств контроля безопасности, направленных на устранение широкого спектра угроз и уязвимостей.

6. Приоритизация средств контроля: Включите концепцию приоритетных элементов управления из CIS Critical Security Controls, предоставляя организациям "дорожную карту" для постепенного повышения уровня безопасности путем систематического и приоритетного внедрения элементов управления.

Преимущества и проблемы принятия гармонизированной системы информационной безопасности. Принятие гармонизированной системы информационной безопасности, которая объединяет ключевые принципы и лучшие практики из ISO/IEC 27001:2013, NIST SP 800-53 и CIS Critical Security Controls, может дать организациям ряд преимуществ и проблем. Согласование этих стандартов может дать ряд преимуществ, включая повышение эффективности, сокращение дублирования усилий, повышение гибкости и лучшее соответствие целям организации [5].

Преимущества:

1. Снижение сложности: Единый подход может помочь уменьшить сложность, связанную с выбором и внедрением нескольких стандартов информационной безопасности, предоставляя организациям единую, всеобъемлющую систему, которой можно следовать.

2. Повышение эффективности: Благодаря интеграции лучших практик из множества стандартов, гармонизированная система может потенциально предложить повышенную эффективность в борьбе с разнообразными и развивающимися киберугрозами.

3. Согласованность и операционная совместимость: Гармонизированная система может способствовать согласованности и операционной совместимости между организациями, облегчая сотрудничество и обмен информацией в сообществе кибербезопасности.

4. Экономия затрат: Организации могут потенциально сэкономить затраты, внедряя единую унифицированную систему вместо инвестиций в несколько стандартов, сокращая время и ресурсы, необходимые для обеспечения соответствия и сертификации.

Сложности:

1. Проблемы внедрения: Интеграция нескольких стандартов в единую унифицированную систему может быть сложным и ресурсоемким процессом, требующим от организаций затрат времени и усилий на разработку и внедрение гармонизированного подхода.

2. Адаптируемость к конкретным отраслевым требованиям: Гармонизированная система может не полностью отвечать уникальным потребностям и требованиям конкретных отраслей или секторов, что потребует дополнительной настройки и адаптации.

3. Сопротивление изменениям: Организации, которые уже внедрили один или несколько существующих стандартов, могут сопротивляться принятию новой, унифицированной системы, поскольку она может потребовать значительных изменений в существующих процессах и практике.

Заключение. Постоянно меняющийся ландшафт киберугроз требует проактивного и адаптивного подхода к информационной безопасности. Гармонизированный подход к стандартам информационной безопасности, объединяющий ключевые принципы и лучшие практики из ISO/IEC 27001:2013, NIST SP 800-53 и CIS Critical Security Controls, может предложить организациям комплексную и целостную структуру для повышения их

киберустойчивости. Хотя принятие единой системы может быть сопряжено с определенными трудностями, потенциальные преимущества в виде снижения сложности, повышения эффективности и экономии средств делают ее перспективным направлением для организаций, стремящихся повысить уровень информационной безопасности в условиях быстро меняющегося ландшафта угроз.

Список литературы:

1. ISO/IEC. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization. Retrieved from https://www.iso.org/standard/54534.html

2. NIST. (2013). NIST Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

3. CIS. (2021). CIS Critical Security Controls. Center for Internet Security. Retrieved from https://www.cisecurity.org/controls/

4. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security.

5. Hentea, M. (2018). A Comparative Analysis of Information Security Standards. Journal of Information Assurance & Security.

6. Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. Cengage Learning.

7. Chapple, M., & Seidl, D. (2019). CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide. John Wiley & Sons.

8. Oueslati, W., & Tounsi, H. (2016). A unified approach for information security management. Journal of Information Security and Applications, 29, 63-77.

9. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102.

10. Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267-270.

11. Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the information security risk assessment process. Software Engineering Institute, Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14857.pdf

12. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-94/final