МЕЖДУНАРОДНЫЕ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И НАЦИОНАЛЬНАЯ ПРАВОВАЯ БАЗА

М. Е. Санаев
Ассистент Самаркандский филиал международной школы финансовых технологий и науки
E-mail: sanayevmashrab@gmail.com

Акбаралиева Гулрух Ахроровна
Самаркандский филиал международной школы финансовых технологий и науки Студент
E-mail: akbaraliyevagulrux7@gmail.com

Международные стандарты в области информационной безопасности

Основная цель стандартов безопасности–создание взаимодействия между производителями продукции информационных технологий, потребителями и экспертами по квалификации.

производителей необходимы для сравнения возможностей информационных продуктов. Кроме того, стандарты необходимы для процедур сертификации, которые рассматриваются как механизм объективной оценки свойств информационной продукции.

Потребители заинтересованы в методе, который позволит им сделать осознанный выбор информационных продуктов в соответствии со своими потребностями. Для этого им нужна шкала рейтинга безопасности.

Эксперты по квалификации продуктов информационных технологий принимают стандарты как инструмент, позволяющий им оценить уровень безопасности, обеспечиваемый продуктами информационных технологий.

Системы управления информационной безопасностью.

Этот стандарт состоит из модели и требований к разработке, внедрению, эксплуатации, мониторингу, анализу, обслуживанию и совершенствованию системы управления информационной безопасностью (СУИБ). Внедрение ISBT должно оставаться стратегическим решением организации. При

разработке и внедрении ISBT следует учитывать потребности безопасности, цели, используемые процессы, размер и структуру организации. Предполагается, что AXBT и поддерживающие его системы со временем изменятся. Также масштаб расширения ISBT будет зависеть от потребностей организации, например, простая ситуация требует простого решения для ISBT. Этот стандарт может использоваться внутренними и внешними сторонами для оценки соответствия.

Процессный подход. Эта стандартная организация ориентирована на использование процессного подхода при разработке, внедрении, эксплуатации, мониторинге, анализе, обслуживании и совершенствовании ISBT.

Для того чтобы организация могла успешно функционировать, она должна идентифицировать и управлять большим количеством взаимосвязанных видов деятельности. Все виды деятельности, в которых используются активы и которые управляются с целью преобразования входных данных в выходные, можно рассматривать как процессы. Часто выходные данные одного процесса создают непосредственные входные данные для следующего процесса.

Процессным подходом можно считать идентификацию системы процессов в организации и их взаимодействие , а также использование системы процессов, а также управление процессами .

Этот подход подчеркивает важность:

- понимать требования организации к информационной безопасности и необходимость установления политики и целей информационной безопасности;
- применение мер управления рисками информационной безопасности организации в общем контексте всех бизнес-рисков ;

показывает, как ISBT использует требования информационной безопасности и ожидаемые результаты заинтересованных сторон в качестве входных данных и получает данные, указывающие на то, что заявленные требования и ожидаемые результаты удовлетворяются за счет реализации необходимого поведения и процессов .

Кроме того, модель PDCA соответствует действующим рекомендациям Организации экономического сотрудничества и развития по безопасности информационных систем и сетей. Этот стандарт предоставляет практическую модель для применения этих принципов к управлению рисками, планированию и реализации безопасности, а также управлению и переоценке безопасности .

1- *пример* Может потребоваться, чтобы нарушение информационной безопасности не могло стать причиной серьезных финансовых потерь и/или каких-либо затруднений для организации .

2- *пример Для серьезного конфликта, например ситуации, возникшей вследствие нарушения сайта организации, осуществляющей электронную коммерцию с использованием сайта, в организации* должны быть специалисты , обладающие достаточными знаниями и опытом для минимизации последствий нарушения . Нарис. 3.1 показано применение модели PDCA к процессам управления персоналом .

этот стандарт позволяет организации адаптировать или интегрировать текущий ISBT с соответствующими требованиями других систем менеджмента.

Практические правила управления информационной безопасностью.

ценный актив, как и любой другой критически важный бизнес-актив , и поэтому она должна быть должным образом защищена. Это особенно важно в постоянно развивающейся бизнес-среде с взаимодействием. Сегодня в результате такого взаимодействия информация подвергается растущему числу и разнообразию угроз и уязвимостей.

быть доступна в различных формах. Оно может быть помещено на бумажный носитель, сохранено в электронном виде, передано по почте или с использованием электронных средств телекоммуникаций, отображено на кинопленке или выражено устно. Независимо от формы доступности информации, способа ее распространения или хранения, она всегда должна быть адекватно защищена.

Информационная безопасность означает защиту информации от широкого спектра угроз для обеспечения непрерывности бизнеса, минимизации бизнес-рисков и максимизации окупаемости инвестиций и возможностей бизнеса.
достигается путем реализации соответствующего набора действий по управлению информационной безопасностью, которые могут обеспечиваться политиками, методами, процедурами, организационными структурами и функциями программного обеспечения. Эти меры должны гарантировать, что организация достигает своих целей информационной безопасности.
Потребность в информационной безопасности. Информация и процессы, которые ее поддерживают, информационные системы и сетевая инфраструктура считаются бесценными активами бизнеса . Выявление, обеспечение, поддержание и улучшение информационной безопасности имеет большое значение для обеспечения конкурентоспособности, ценности, прибыльности, соблюдения законодательства и деловой репутации организации.
Организации, их информационные системы и сети все чаще сталкиваются с угрозами безопасности, такими как компьютерное мошенничество, фишинг , вредоносное ПО, вандализм, пожары или наводнения. Источники ущерба, такие как компьютерные вирусы, компьютерный взлом и атаки типа «отказ в обслуживании» , становятся все более распространенными, агрессивными и изощренными.
Информационная безопасность важна в государственном и частном секторах бизнеса, а также в защите критически важных инфраструктур. Информационная безопасность должна помочь в обоих секторах, например, избежать или снизить риски, связанные с внедрением электронного правительства или электронного бизнеса. Совместная работа публичных и частных сетей, а также совместное использование информационных ресурсов затрудняет контроль за использованием информации. Тенденция к использованию распределенной обработки данных ослабляет эффективность централизованного управления.
Вопросы безопасности не учитывались при проектировании многих информационных систем. Уровень безопасности, которого можно достичь

техническими средствами, имеет ряд ограничений и поэтому должен обеспечиваться соответствующими средствами контроля и процедурами. Выбор необходимых мероприятий по управлению информационной безопасностью требует тщательного планирования и детализации.

Управление информационной безопасностью требует как минимум участия всех сотрудников организации. Также может потребоваться участие поставщиков, клиентов или акционеров. Кроме того, может потребоваться экспертная консультация сторонних организаций .

мероприятия по управлению информационной безопасностью включить в техническое задание на этапе проектирования информационной системы, это будет значительно дешевле и эффективнее.

Определение требований информационной безопасности. Для организации важно определить свои требования к информационной безопасности, принимая во внимание следующие три важных фактора:

- с учетом глобальной стратегии бизнеса и целей организации выявляются угрозы активам организации с использованием оценки рисков организации, уязвимости соответствующих активов и вероятности возникновения угроз , как а также оцениваются возможные последствия;
- в качестве другого фактора рассматриваются организация, ее торговые партнеры, подрядчики и поставщики услуг, требования законодательства , требования правовых документов, нормативные и договорные требования, а также социокультурная среда этих сторон;
- еще одним фактором является особый набор принципов, целей и требований, разработанных организацией для обеспечения ее функционирования.

Оценка рисков информационной безопасности. Требования информационной безопасности определяются с помощью регулярных оценок рисков. Затраты на деятельность по управлению информационной безопасностью должны быть пропорциональны размеру ущерба, который может быть причинен организации в результате нарушений информационной безопасности.

Результаты данной оценки помогут определить конкретные меры и приоритеты в области управления рисками информационной безопасности , а также реализации мероприятий по управлению информационной

безопасностью в целях минимизации этих рисков. Анализ рисков следует периодически пересматривать, чтобы учитывать любые изменения, которые могут повлиять на эффективность существующих мер .

мероприятий по управлению информационной безопасностью . После определения требований информационной безопасности и выявления рисков следует выбрать и реализовать меры управления информационной безопасностью, чтобы гарантировать снижение рисков до приемлемого уровня. Эти действия могут быть выбраны из настоящего стандарта или других источников, а действия могут быть разработаны для удовлетворения конкретных потребностей организации в области управления информационной безопасностью. Выбор мероприятий по управлению информационной безопасностью зависит от критериев принятия рисков, организационных решений, основанных на вариантах оценки рисков, и общего подхода к управлению рисками, принятого в организации. Этот выбор должен быть скоординирован с эквивалентным национальным и международным законодательством и нормами.

в этом стандарте, могут быть приняты в качестве применимых принципов управления информационной безопасностью и применимы ко многим организациям. Такая деятельность более подробно обсуждается ниже в разделе «Фокус на обеспечении информационной безопасности» .

Ориентир для реализации информационной безопасности. Отдельные меры управления информационной безопасностью могут быть приняты в качестве применимых принципов управления информационной безопасностью и служить отправной точкой для ее реализации. Такие меры основаны на основных требованиях законодательства или могут быть приняты как общепринятая практика в сфере информационной безопасности.

обеспечения информационной безопасности с точки зрения законодательства являются:

- защита данных и конфиденциальность личной информации;
- защита организационных документов;
- права интеллектуальной собственности.

Деятельность по управлению информационной безопасностью, считающаяся общепринятой практикой в области информационной безопасности, включает в себя:

- документирование политики информационной безопасности;
- по обеспечению информационной безопасности ;
- обучение информационной безопасности ;
- корректная обработка информации в приложениях ;
- стратегия управления техническими уязвимостями;
- управление непрерывной работой организации;
- управление инцидентами и улучшениями информационной безопасности.

Перечисленные действия могут быть применены ко многим организациям и информационным средам. Хотя все меры, изложенные в настоящем стандарте, считаются важными, целесообразность любой меры должна определяться с учетом конкретных рисков, с которыми сталкивается организация. Поэтому, хотя описанный выше подход и считается отправной точкой реализации мер информационной безопасности, он не заменяет выбор мер управления информационной безопасностью на основе оценки рисков.

Наиболее важные факторы успеха. Опыт показывает , что решающими для успешной реализации мер информационной безопасности в организации являются следующие факторы:

- согласование целей, политик и процедур информационной безопасности с бизнес-целями;
- внедрению, поддержке, мониторингу и модернизации системы безопасности ;
- реальная поддержка и интерес со стороны руководства ;
- четкое понимание требований безопасности, оценки рисков и управления рисками;
- эффективный маркетинг информационной безопасности руководителями и сотрудниками организации , а также обеспечение понимания необходимости применения мер информационной безопасности;
- инструкций, рекомендаций и соответствующих стандартов, связанных

с политикой информационной безопасности, всем сотрудникам и субподрядчикам;

- деятельности по управлению информационной безопасностью ;
- обеспечить необходимый уровень образования и подготовки ;
- подтвердить эффективный процесс управления конфликтами информационной безопасности;
- комплексная и сбалансированная система измеримых показателей, используемых для оценки эффективности управления информационной безопасностью, и предложений исполнителей по ее совершенствованию .

Разработка инструкций, связанных с организацией. Этот стандарт следует рассматривать как отправную точку для разработки руководств для конкретных нужд организации. Не все рекомендации и меры, содержащиеся в настоящем стандарте, будут применимы.

Кроме того, могут потребоваться дополнительные меры, не включенные в настоящий стандарт. В этом случае может оказаться полезным хранить отзывы от нескольких сторон одновременно, что облегчает проверку соответствия со стороны аудиторов и деловых партнеров.

Список использованных литератур

1. Ergashevich, E.A. (2017). Implementation of Modern Pedagogical Technologies in the Process of Training Sessions.Asian Journal of Multidimensional Research (AJMR),6(5), 37-47.
2. Ernazarov, A.E. Specific features of training.International Journal on Integrated Education,3(5), 30-34.
3. Eshquvvat o’g’li M.S, Zafar qizi Z.B AREAS OF APPLICATION OF ARTIFICIAL INTELLIGENCE ISSN: 2181-4027 SJIF: 4.995 Volume-27, Issue-2, February-2023. 61-64.
4. Eshquvvat o’g’li M.S, Naim o‘g‘li M. D, Xamrobek o’g’li N.N, DATA MININGDA CRISP-DM METODOLIGIYASI TASNIFI Часть-11 Том-1 Декабрь-2023 43-46.
5. Файзиев Б.М, Бегматов Т.И, Санаев М.Э. ОБРАТНАЯ ЗАДАЧА ПО ОПРЕДЕЛЕНИЮ КИНЕТИЧЕСКОГО КОЭФФИЦИЕНТА В МОДЕЛИ

ФИЛЬТРАЦ II TOM TATU SF MA'RUZALAR TO'PLAMI 9 aprel 2022-yil 11-13.

6. Файзиев Б.М, Бегматов Т.И, Санаев М.Э. ИДЕНТИФИКАЦИЯ КОЭФФИЦИЕНТА КИНЕТИКИ В МОДЕЛИ ФИЛЬТРАЦИИ СУСПЕНЗИИ В ПОРИСТОЙ СРЕДЕ ХАЛҚАРО ИЛМИЙ-АМАЛИЙ АНЖУМАН МАТЕРИАЛЛАРИ 2022 йил, 11-12 май 360-361.

7. Eshquvvat o'g'li.M.S, Shodiyor o'g'li.Sh.J, Raxmonqul o'g'li.A.T, MA'LUMOTLARNI SINFLASHTIRISHDA BIRCH ALGORITMI AHAMIYATI Часть-11 Том-1 Декабрь -2023 39-42.

8. Eshquvvat o'g'li.M.S, Elmurza o'g'li.Z.B, Anvar o'g'li.B.A DATA MININGDA SEMMA METODOLIGIYASI TASNIFI Часть-11_ Том-1_ Декабрь -2023 35-38.

9. Eshquvvat o'g'li.M.S, MA'LUMOTLARNI SINFLASHTIRISHDA BIRCH ALGORITMI AHAMIYATI Часть-11 Том-1 Декабрь -2023 39-42.

10. ME Sanayev METHOD ORIENTED PRACTICAL SOFTWARE CLASSIFICATION

11. Eshquvvat o'g'li.M.S, DATA MININGDA SEMMA METODOLIGIYASI TASNIFI Часть-11 Том-1 Декабрь -2023 35-38

12. Ergashevich, E. A. (2024). FORMS OF ORGANIZING STUDENTS'ACTIVITIES AND COMPONENTS OF COURSE RAINING. *Excellencia: International Multi-disciplinary Journal of Education (2994-9521)*,*2*(1), 292-300.

13. Ergashevich, E. A. (2024). Analysis of the Use of Modern Educational Clubs and Technologies in Educational Courses.*EUROPEAN JOURNAL OF INNOVATION IN NONFORMAL EDUCATION*,*4*(1), 62-63.

14. SM Eshquvvat o'g'li DATA MININGDA PMML STANDARTI Лучшие интеллектуальные исследования 11 (1), 47-50