Научная статья
УДК 34:004:34.05:004.056.5
EDN: https://elibrary.ru/xujvtm
DOI: https://doi.org/10.21202/jdtl.2025.6

Универсальная система управления информационной безопасностью: организационно-правовые принципы

Мусадак Ахмед Хади ✉

Технологический университет, Багдад, Ирак

Мохаммед Наджм Абдулредха

Багдадский университет, Багдад, Ирак

Ключевые слова

законодательство,
защита информации,
информационная безопасность,
информационные технологии,
кибербезопасность,
организационная структура,
право,
правовое регулирование,
управление информационной безопасностью,
цифровые технологии

Аннотация

Цель: разработка универсальных организационно-правовых принципов построения системы управления информационной безопасностью, которые позволят каждой организации создать собственную эффективную систему управления информационной безопасностью с учетом ее уникальных бизнес-целей и задач.

Методы: основаны на интеграции ключевых элементов управления информационной безопасностью, таких как видение, стратегия, цели, политики, стандарты, процессы и матрицы. Видение и цели задают направление развития организации, политики и стандарты обеспечивают концептуальную основу для защиты информации, процессы позволяют систематически достигать поставленных задач, а матрицы предоставляют инструменты для оценки и контроля всей структуры. Предложенные принципы согласуются с международными стандартами, нормативными требованиями и лучшими практиками в области информационной безопасности.

Результаты: разработанная система управления информационной безопасностью позволяет четко распределить роли и обязанности среди сотрудников организации, обеспечивая эффективное внедрение системы управления. Авторы также анализируют существующие принципы безопасности информационных технологий, интегрируя их в стратегию безопасности, которая соответствует целям организации. Предложенная универсальная система соответствует нормативным правовым требованиям и может быть адаптирована для использования в организациях любого масштаба и профиля.

✉ Контактное лицо

Научная новизна: заключается в представлении практического подхода к внедрению системы управления информационной безопасностью, основанного на опыте авторов, а также на мировых стандартах, системах контроля и правовых актах. В отличие от существующих подходов предлагаемая система является гибкой и может быть адаптирована под специфику любой организации, что делает ее универсальным инструментом для управления информационной безопасностью.

Практическая значимость: состоит в предоставлении структурированного подхода к созданию универсальной системы управления информационной безопасностью, который может быть использован организациями, испытывающими недостаток знаний и ресурсов для реализации подобных инициатив. Авторы предлагают общую структуру, которая может быть адаптирована в зависимости от активов организации, уровня подготовки сотрудников и их осведомленности в вопросах информационной безопасности. Это делает настоящую работу ценным ресурсом для специалистов, стремящихся повысить уровень защиты информации в своих организациях

Для цитирования

Хади, М. А., Абдулредха, М. Н. (2025). Универсальная система управления информационной безопасностью: организационно-правовые принципы. *Journal of Digital Technologies and Law*, *3*(1), 125–142. https://doi.org/10.21202/jdtl.2025.6

Содержание

Введение

Информационная безопасность зародилась еще в древние времена, когда египтяне, греки и римляне применяли методы защиты сообщений, например, криптографию. Одним из первых и самых известных людей, защищавших сообщения, был Юлий Цезарь. Он изобрел и использовал шифр Цезаря для защиты своих личных сообщений в военных целях. С тех пор многое было сделано для решения этой проблемы, и теперь ею занимаются организации, в обязанности которых входит обеспечение информационной безопасности. В Средние века было изобретено множество методов защиты данных, например, стеганография, которая основана на сокрытии факта передачи сообщения (Rao & Nayak, 2014; Hadi et al., 2023; Wu et al., 2021).

В 1889 г. британское правительство приняло Закон о государственной тайне, заложив принципы классификации для защиты конфиденциальных данных. Кроме того,

в 1919 г. были созданы государственные кодексы безопасности. Они применялись во время Первой мировой войны для обеспечения безопасности передачи секретных данных. К этому времени было изобретено множество методов и алгоритмов защиты, таких как алгоритмы классификации, алгоритмы криптографии, алгоритмы взлома кодов (Ohki et al., 2009).

Во время Второй мировой войны немцы спроектировали и создали одно из самых важных устройств для защиты информации – «Энигма». Это электромеханическое устройство использовалось для шифрования и дешифрования сообщений о военных действиях. Математик и криптоаналитик Алан Тьюринг, работавший в Британской правительственной школе кодов и шифров, разгадал немецкий код и расшифровал его. В эту эпоху было сделано множество технологических достижений в области информационной безопасности, защиты связи, шифрования и компьютерных наук, которые облегчили обмен информацией и конфиденциальными данными (Rastogi & von Solms, 2005).

В период с 1960 по 1990 г. сфера информационной безопасности значительно продвинулась в связи с развитием цифровых электронных и информационных технологий. В этот период были изобретены первые мейнфреймовые компьютеры; системы с разделением времени получили большее значение с развитием механизмов защиты данных. Кроме того, развитие сетевых комплексов ARPANET сопровождалось разработкой стандарта шифрования данных (Data Encryption Standard, DES) на основе симметричного ключа. Затем на сцену вышли локальные сети (Local Area Networks, LAN) и персональные компьютеры (PC), а организации начали внедрять системы обнаружения вторжений (Intrusion Detection Systems, IDS), системы предотвращения вторжений (Intrusion Prevention Systems, IPS) и межсетевые экраны для защиты информации в сетях. К концу 1980-х гг. информационная безопасность стала важным аспектом компьютерных и сетевых операций, что заложило основу для эры кибербезопасности[1] (Bendovschi, 2015; Johnston & Hale, 2009).

С 1990 по 2024 г. информационная безопасность стремительно развивалась благодаря расширению концепций безопасности и средств защиты. Основной причиной этого стало изобретение Интернета в 1990-х гг., которое поставило сложные задачи в сфере информационной безопасности, например, преобразование обычных протоколов в защищенные (HTTP в HTTPS) путем добавления протоколов безопасности (SSL). Кроме того, появились новые технологии, такие как IoT, блокчейн, облачные вычисления, квантовые компьютеры и искусственный интеллект. Это породило множество векторов атак, включая кибератаки, что усложнило достижение информационной безопасности организации. В результате для обеспечения безопасности данных каждая организация должна была разработать и внедрить собственную систему управления информационной безопасностью (далее – УИБ) (Corriss, 2010; Moulton & Coles, 2003; AlGhamdi et al., 2020).

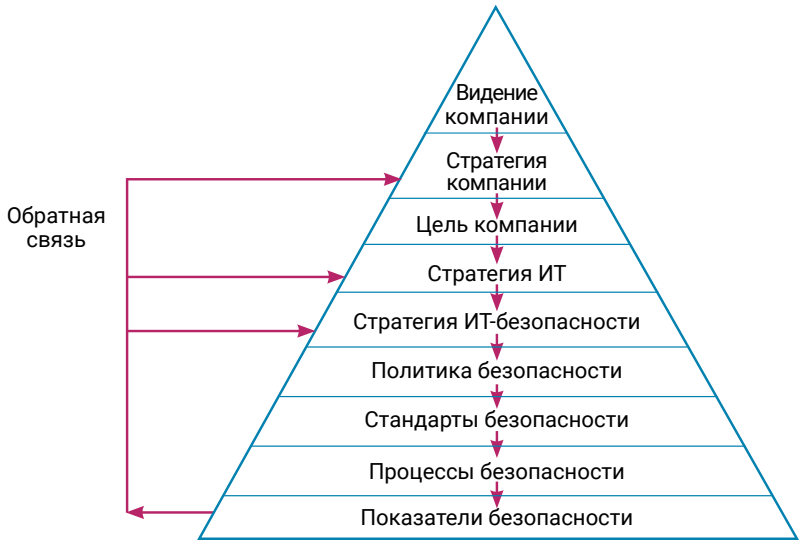
В настоящее время основным направлением деятельности в области информационной безопасности является управление всеми активами, такими как люди, риски, инциденты, уязвимости, а также планирование обеспечения непрерывности бизнеса. С другой стороны, для измерения и оценки с целью достижения эффективности программы УИБ, а также улучшения деятельности организации, используются метрики и другие инструменты мониторинга процессов и процедур. Однако информационную безопасность необходимо рассматривать как важнейшую бизнес-задачу,

[1] Gregory, P. H. (2018). CISM®: Certified Information Security Manager Exam Guide. New York: McGraw Hill Education.

поскольку отсутствие защиты данных приводит к серьезным проблемам в организациях. Это свидетельствует о недостаточности понимания и знаний у высшего руководства и советов директоров. Кроме того, государственные и частные организации сталкиваются с проблемами обеспечения информационной безопасности на уровне совета директоров из-за недостатка знаний или навыков в области кибербезопасности[2] (Carcary et al., 2016; Rocha Flores et al., 2014).

В первую очередь сотрудники, руководители и члены совета директоров должны понимать важность наличия УИБ, иначе ее невозможно будет эффективно применять. Во-вторых, для успешного внедрения УИБ должна существовать надежная программа управления сектором ИТ. Адекватная структура УИБ должна быть поддержана адекватной структурой ИТ, и они должны быть интегрированы для достижения целей и задач организации. В стратегическом плане система ИТ помогает деятельности организации, поддерживая операционную эффективность. Архитектура системы УИБ предлагает высокоорганизованный метод контроля за ИТ-процессами и активами. В конечном итоге, проще говоря, сотрудничество в управлении УИБ и IT необходимо для того, чтобы гарантировать, что информационная безопасность государственных и частных организаций не только присутствует, но и согласуется с их общими бизнес-целями (S. H. von Solms & R. von Solms, 2010).

В настоящей статье предлагается эффективная система УИБ (включая кибербезопасность) для государственных и частных организаций, которая поможет им защищать и контролировать свои активы и ИТ-сектор. Поскольку информационная безопасность подразумевает защиту всех форм информации, кибербезопасность – это одно из направлений информационной безопасности, направленное на защиту цифровой информации. Поэтому все, что применяется в рамках УИБ, обязательно включает в себя средства обеспечения кибербезопасности. Более того, предлагаемая ниже структура УИБ должна работать в соответствии с законами и правилами, что делает ее реализацию последовательной (рис.). В конечном счете управление ИТ-сектором и УИБ должно осуществляться в сотрудничестве, что упростит его и сделает более отвечающим потребностям организации.



Концептуальная структура организации
Источник: (H., von S.S. & Solms, 2010).

[2] Gregory, P. H. (2022). CISM Certified Information Security manager all-in-one exam guide. New York: McGraw Hill.

Данная работа построена следующим образом. В разделе 1 изложен ключевой вопрос о целях и задачах создания системы УИБ и ее подробное описание. В разделе 2 представлены роли и обязанности сотрудников с матрицей распределения ответственности RACI и составляющими элементами организации. В разделе 3 описаны лучшие образцы УИБ в качестве основы для разработки индивидуальной системы УИБ. В разделе 4 представлены предлагаемая структура УИБ, регулирующие законы и нормы, а также действия организации по внедрению системы УИБ.

1. Почему организации должны иметь систему управления информационной безопасностью?

В данном разделе представлены потребности, обязательно присутствующие у организаций, имеющих собственную систему УИБ. В целом УИБ необходима государственным и частным организациям в связи с быстрым развитием технологий и социальных сетей, о чем говорилось во введении. Таким образом, деятельность многих государственных организаций в различных секторах существенно зависит от их информационной и ИТ-инфраструктуры. Эта зависимость может достигнуть уровня, когда для поддержания своей деятельности организация должна будет сосредоточиться на продуктах/услугах, связанных с информацией. Организациям также необходимо будет обеспечить безопасность своих активов и данных, учитывая приоритетность их сферы деятельности и применяя принципы конфиденциальности, целостности и доступности (Confidentiality, Integrity, and Availability, CIA)[3].

Цель разработки системы УИБ – удовлетворить потребности бизнеса, включая стратегию обеспечения и эффективного контроля информационной безопасности. Кроме того, при этом устанавливаются формальные средства контроля безопасности, обеспечивающие деятельность и ее желаемые результаты. Программы секторов ИТ и безопасности структурируются и выполняются последовательно, что отвечает приоритетам бизнеса. При этом формальные средства контроля и измерения процессов дают руководству четкое представление о том, как организация управляет безопасностью. Эффективность программы УИБ обеспечивается путем согласования управления безопасностью с процедурами, которые используются в корпоративном и ИТ-управлении. Управление безопасностью должно быть интегрировано в процессы ИТ и корпоративного управления. В конечном итоге благодаря управлению безопасностью и стратегическому планированию предлагаемая система УИБ может обеспечить общее управление как в государственных, так и в частных организациях (Rebollo et al., 2015).

Итак, для эффективного внедрения системы УИБ руководители высшего звена организации должны взять на себя ответственность за защиту данных в своих организациях. Вот некоторые виды деятельности, которые должны быть включены в рамочную программу УИБ организации (Rebollo et al., 2015):

а) управление рисками: необходимо управлять рисками организации, чтобы смягчить существующие и будущие риски. Однако в некоторых случаях руководство должно пойти на компромисс и принять определенный уровень риска для поддержания функциональности организации;

[3] Gregory, P. H. (2020). CISA Certified Information Systems Auditor all-in-one exam guide. New York: McGraw-Hill.

б) соответствие: организация должна действовать в соответствии с законами и нормативными актами, действующими в стране, а также иметь собственные стандарты для защиты своих данных и активов;

в) управление реагированием на чрезвычайные ситуации: руководители организации должны разработать стратегию работы с чрезвычайными ситуациями, чтобы контролировать внезапные события, минимизировать их последствия и поддерживать возможности организации по смягчению последствий;

г) план обеспечения непрерывности бизнеса (далее – ПНБ), гарантирующий, что организация будет продолжать функционировать во время и после любой чрезвычайной ситуации или бедствия. Кроме того, он включает в себя план аварийного восстановления (далее – ПАВ) для поддержания деятельности организации;

д) план аварийного восстановления: это часть ПНБ, которая направлена на восстановление данных, инфраструктуры, ИТ-систем организации после чрезвычайной ситуации или бедствия. В ПАВ должна быть предусмотрена команда экстренной помощи, которая создает резервные копии (зеркала), различные сайты (горячий, холодный) и документацию;

е) осведомленность о безопасности: важно поддерживать определенный уровень осведомленности всех членов организации об информационной безопасности и о том, что дает система УИБ, путем проведения различных обучающих программ в течение всего года, особенно для ИТ-сектора и управленческого персонала.

Благодаря этой деятельности руководители высшего звена занимают активную позицию в управлении и руководстве информационными системами организации, обеспечивая устойчивость к потенциальным угрозам и развивая стратегический подход к управлению безопасностью.

2. Должности, роли и зоны ответственности в организации

Отдел информационной безопасности в любой организации воспринимается как «все запрещающий» и препятствующий ведению бизнеса. Такой образ сложился благодаря тому, что его руководители иногда проявляют чрезмерную осторожность в отношении рисков, ограничивают расширение организации, внедрение инновационных продуктов и услуг. В результате такая репутация порождает у персонала ИТ-сектора и других подразделений нежелание взаимодействовать со специалистами по безопасности; они опасаются, что сотрудничество может помешать их работе. Более того, признаком правильного внедрения системы УИБ служит то, что работники организации понимают свои обязанности, роли и зону ответственности и четко их придерживаются. Поэтому организациям следует установить формальные роли и обязанности, в соответствии с которыми каждый сотрудник должен получить инструкции по сохранению данных и активов организации. Эти роли должны быть связаны с названиями должностей, указывая на место сотрудника в организации. Названия должностей нужны в организациях, чтобы гарантировать, что каждый сотрудник работает в соответствии со своими должностными обязанностями. Как правило, названия должностей связаны с позицией сотрудника, которая отражает уровень его полномочий. Вот некоторые названия должностей, перечисленные в порядке старшинства (Nicho, 2018):

а. Председатель совета директоров.

б. Член совета директоров.

в. Главный исполнительный директор.

г. Президент.
д. Исполнительный вице-президент.
е. Старший вице-президент.
ж. Вице-президент.
з. Исполнительный директор.
и. Старший директор.
к. Директор.
л. Старший менеджер.
м. Менеджер.
н. Супервайзер.

В приведенном списке показаны некоторые ранги иерархии, но в крупных организациях существуют и другие должности, такие как первый вице-президент, генеральный директор или помощник директора. Кроме того, обязанности во многом похожи на роли, определяющие задачи, выполнения которых ожидают от сотрудника. В целях информационной безопасности организации распределяют конкретные роли и обязанности между сотрудниками, что гарантирует выполнение стратегии и целей организации в области ИБ.

2.1. Стандартный метод управления организациями

Многие организации используют собственные методы управления информационной безопасностью, например, проводят различные меры в этой области. Однако существует стандартный метод, который широко используется для определения ролей и обязанностей в организациях, – матрица распределения ответственности RACI (Responsible – Accountable – Consulted – Informed). Она служит для распределения ролей между сотрудниками и командами для выполнения задач и действий. Кроме того, матрица в общих чертах описывает, кто и что должен делать в данной организации. Например, менеджер проекта должен также выполнять обязанности аналитика по безопасности. Кроме того, согласно матрице RACI обязанности каждого сотрудника на любом уровне старшинства распределяются следующим образом (Bettwy et al., 2016):

i. Исполнитель: сотрудник, который отвечает за непосредственное выполнение задания.

ii. Ответственный: сотрудник, который руководит работой исполнителя и отвечает за результат выполнения задания.

iii. Консультант: специалист либо эксперт в предметной области, с которым можно проконсультироваться по какому-либо вопросу.

iv. Наблюдатель, информируемое лицо: сотрудник, которого надлежит уведомлять во время или до начала действия.

В табл. 1 приведен пример распределения ролей и обязанностей в организации. Прежде всего, каждый сотрудник в организации должен иметь должность и принадлежать к тому или иному подразделению. Кроме того, все сотрудники должны пройти специальный курс обучения, который даст им набор навыков для выполнения поставленных задач. Согласно матрице RACI, каждый сотрудник имеет свои собственные задачи, что и называется разделением обязанностей (Separation of Duties, SoD). SoD означает, что ни один сотрудник не имеет полного контроля над критическим процессом деятельности, который может повлиять на функциональность организации. Например, при предоставлении сотруднику учетной записи лицо, предоставляющее,

утверждающее и запрашивающее данные, не должно принадлежать к тому же отделу в целях предотвращения конфликта интересов (Von Solms et al., 2011).

Таблица 1. Распределение ролей и обязанностей в матрице RACI

Деятельность	Исполнитель	Ответственный	Консультант	Наблюдатель
Контроль аккаунта пользователя	IA	IAM	AO	IT SD, IT SM, EUM
Предоставление аккаунта пользователя	IT SD	IT SM	AO	IT SD, EUM, ST
Утверждение аккаунта пользователя	AO	COO	EUM, ST	EU, IA, IT SD
Запрос на аккаунт пользователя	EU	EUM	IT SD, EUM	AO, ST

* EU – конечный пользователь, EUM – менеджер конечного пользователя, SD – отдел обслуживания, AO – владелец активов, ST – отдел безопасности, IA – внутренний аудит, SM – менеджер по обслуживанию, IAM – менеджер внутреннего аудита.

Источник: (Von Solms et al., 2011).

2.2. Стандарты и принципы безопасности в организациях

Успешная организация действует в рамках правильно разработанной системы УИБ, основанной на стандартах, которые соответствуют ее видению и стратегии. Однако не так-то просто разработать стратегию, которая включала бы в себя политику компании, стандарты, процессы и матрицы в соответствии с общим видением организации. В данном разделе представлены стандарты, которые применяются в таких организациях мирового масштаба, как Google, Meta[4], Amazon и т. д. Более того, если специалист по безопасности вместе с руководителями высшего звена решают разработать структуру УИБ для своей организации и ограничиваются только системой контроля, это считается ошибкой. Мы предлагаем использовать данную структуру УИБ в качестве примера и изучить мировые стандарты и средства контроля безопасности, чтобы избежать ошибок и обеспечить хороший старт в управлении организацией. В табл. 2 перечислены стандарты и системы контроля, которые могут быть полезны в качестве отправной точки для разработки системы УИБ для государственных и частных организаций (Tan et al., 2010; Fazlida & Said, 2015; Ula et al., 2017).

Таблица 2. Некоторые стандарты и принципы контроля

№	Стандарты и принципы	Пояснение
1	Национальный институт стандартов и технологий (National Institute of Standards and Technology, NIST)	Используется Министерством торговли США для стандартизации в области экономической безопасности, инноваций, промышленности и технологий
2	Международная организация по стандартизации/Международная электротехническая комиссия (International Organization for Standardization/ International Electrotechnical Commission, ISO/IEC)	Два основных международных стандарта в области информационной безопасности, технологий, промышленности и деловой практики

[4] Организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

Окончание табл. 2

№	Стандарты и принципы	Пояснение
3	Контрольные точки в области информационных и смежных технологий (Control Objectives for Information and Related Technologies, COBIT)	Система управления сектором ИТ и предприятиями, которая устанавливает ряд руководящих принципов и лучшие практики для ИТ-организаций
4	Стандарт безопасности данных в области платежных карт (Payment Card Industry Data Security Standard, PCI-DSS)	Стандарты информационной безопасности, разработанные для защиты конфиденциальной информации платежных карт
5	Закон о переносимости и подотчетности в сфере медицинского страхования (Health Insurance Portability and Accountability Act, HIPAA)	Закон США, защищающий конфиденциальность информации о здоровье людей и обеспечивающий безопасность медицинских данных
6	Форум по информационной безопасности (Information Security Forum, ISF)	Набор средств контроля безопасности и лучших практик, используемых для управления рисками в сфере информационной безопасности
7	Библиотека инфраструктуры информационных технологий (Information Technology Infrastructure Library, ITIL)	Система ИТ-услуг, разработанная для целей управления, включая управление ИТ-инфраструктурой, средой, услугами и процессами

Источник: (Ula et al., 2017).

3. Лучшие системы управления информационной безопасностью

В данном разделе представлен ряд ведущих систем в области УИБ и кибербезопасности. Такие системы есть и в арабских странах. Например, Объединенные Арабские Эмираты и Саудовская Аравия являются примером для подражания в этой важной области. Ниже перечислены системы УИБ, законы и правила контроля информации ряда стран (Shingarev & Kazakova, 2021; Creemers, 2023; Priyadarshini & Cotton, 2022; Carr & Tanczer, 2018; Singh & Alshammari, 2020; Al Neaimi et al., 2015):

а) Россия: в систему входит Федеральная служба по техническому и экспортному контролю (ФСТЭК), обеспечивающая безопасность продукции; действует Федеральный закон № 149-ФЗ для защиты данных; важную роль в обеспечении кибербезопасности играет Федеральная служба безопасности (ФСБ). Согласно законодательству, информация российских граждан должна храниться внутри страны (Shingarev & Kazakova, 2021);

б) Китай: в систему УИБ входит Министерство общественной безопасности (МОБ), которое следит за информационной безопасностью в Китае. Кроме того, в 2017 г. в Китае приняты Закон о кибербезопасности и Закон о национальной безопасности (NSL), а также Закон об управлении киберпространством Китая (CAC), который регулирует работу Интернета (Creemers, 2023);

в) США: система УИБ включает Федеральный закон об управлении информационной безопасностью (FISMA) и Закон о повышении кибербезопасности (CEA) от 2014 г. Кроме того, действует Национальный институт стандартов и технологий (NIST), который устанавливает стандарты. Агентство по кибербезопасности и инфраструктурной безопасности (CISA) координирует деятельность таких структур, занимающихся вопросами кибербезопасности, как Агентство национальной безопасности (АНБ) (Priyadarshini & Cotton, 2022);

г) Великобритания: система УИБ включает акты и стратегии Национальной стратегии кибербезопасности (NCSC) и Закон о защите данных (DPA) 2018 г. Кроме того, Закон о неправомерном использовании компьютеров (CMA) 1990 г. предусматривает киберпреступления. Правительство Великобритании участвует в международном сотрудничестве в области кибербезопасности (Carr & Tanczer, 2018);

д) Саудовская Аравия: система УИБ включает Закон о кибербезопасности Саудовской Аравии (SACL) от 2019 г., который контролируется Комиссией по коммуникациям, космосу и технологиям (CITC) и Национальным управлением по кибербезопасности (NCA). Центральный банк Саудовской Аравии (SAMA) осуществляет надзор за операциями в финансовом секторе (Singh & Alshammari, 2020);

е) ОАЭ: система УИБ включает Закон о кибербезопасности ОАЭ от 2019 г. и надзор со стороны Национального управления электронной безопасности (NESA) и Управления по регулированию телекоммуникаций и цифрового управления (TRDA). Вопросами надзора за кибербезопасностью в Дубае занимается Дубайский англоязычный колледж (DESC) (Al Neaimi et al., 2015).

4. Предлагаемая система управления информационной безопасностью

Прежде чем предлагать какую-либо новую систему или развивать существующую, необходимо объяснить сущность двух фундаментальных понятий: управления и корпоративного управления. Управление связано с защитой интересов собственников путем руководства, управления и надзора от их имени, при этом совет директоров выступает в качестве их представителей. Корпоративное управление определяется как реакция на различия интересов руководства и собственников в частных и государственных организациях. Кроме того, оно направлено на поддержание этого различия через стимулирование руководства и совета директоров преследовать цели, которые соответствуют интересам компании и ее акционеров.

Предлагаемая структура УИБ должна включать ряд элементов, обеспечивающих эффективную защиту и управление информационными активами организации, обеспечение дисциплины собственников и руководства, а также предоставление собственникам полномочий по контролю за деятельностью организации. Кроме того, создавая безопасную среду для обмена и хранения информации, организации могут не только повысить производительность, потребительские преимущества и эффективность бизнеса, но и обеспечить меры безопасности. И наоборот, любая небезопасная рабочая среда представляет собой значительный риск, который может нанести существенный ущерб корпорациям и правительствам, а также негативно отразиться на гражданах и потребителях. Это особенно важно для предприятий, работающих в таких критически важных сферах, как финансы, электроэнергетика, банковское дело или здравоохранение, где ставки исключительно высоки. В табл. 3 показаны основные вопросы организации эффективной системы УИБ.

Таблица 3. Основные вопросы/действия по организации эффективной системы УИБ

Действующие лица/ Действия	Руководитель предприятия	Руководитель подразделения	Старший управляющий	ИТ-директор/директор по информационной безопасности
Управление/движущие силы бизнеса	Что от меня требуется? Что я должен обязательно сделать?			
Роли и ответственность	Как я могу выполнить свои задачи?			
Измерения/Аудит	Насколько эффективно я могу выполнить свои задачи? Что я должен изменить?			

Система УИБ служит инструментом реализации стратегии и видения руководителей высшего звена для достижения высокой эффективности бизнес-операций и принятия решений в организациях. В их компетенцию входят управление всей деятельностью организации и защита ее данных и активов путем обеспечения эффективной интеграции информационной безопасности в масштабах всей организации.

Чтобы разработать эффективную систему УИБ, которая может быть утверждена и принята во всем мире, необходимо принять во внимание ряд глобальных законов и норм. Они могут дать большое преимущество благодаря своей структуре и продуманности, если опираться на них как на законодательный опыт других стран. В табл. 4 приведены некоторые ключевые законы и нормы, которые использовались в разных странах мира для регулирования информационной безопасности.

Таблица 4. Примеры законов и нормативных актов, принятых в разных странах мира[5]

№	Законы и нормы	Пояснения
1	Общий регламент по защите данных (General Data Protection Regulation, GDPR)	Обязывает организации защищать личные данные граждан на территории Европейского союза и устанавливает строгие требования к конфиденциальности и безопасности данных
2	Закон Калифорнии о защите персональных данных потребителей (California Consumer Privacy Act, CCPA)	Распространяется на компании, которые собирают личную информацию жителей Калифорнии, и требует принятия мер по защите конфиденциальности и безопасности такой информации
3	Закон Сарбейнса – Оксли (Sarbanes – Oxley Act, SOX)	Требует создания и поддержания внутреннего контроля над финансовой отчетностью компаний, включая меры по защите целостности и конфиденциальности финансовых данных
4	Федеральный закон об управлении информационной безопасностью (Federal Information Security Management Act, FISMA)	Федеральный закон США, который устанавливает требования безопасности для федеральных информационных систем и обеспечивает основу для управления рисками кибербезопасности в федеральных агентствах
5	Сертификация модели кибербезопасности (Cybersecurity Maturity Model Certification, CMMC)	Разработана Министерством обороны США для оценки и повышения уровня кибербезопасности подрядчиков и субподрядчиков оборонной отрасли
6	Законы о защите данных (Data Protection Laws, DPL)	В разных странах приняты свои законы о защите данных, например, Закон о защите персональной информации и электронных документов (PIPEDA) в Канаде и Закон о защите персональных данных (PDPA) в Сингапуре

Заключение

В данной работе предлагается новая система УИБ (включая кибербезопасность) для защиты информации и активов государственных и частных организаций, использующая преимущества ряда законов и нормативных актов. Эту систему можно сравнить с существующими системами, которые были внедрены в организациях по всему миру. Она нацелена на достижение баланса между постоянным совершенствованием и управлением рисками и соответствует бизнес-модели организации, основанной на требованиях нормативных актов и законов. Подчеркивается,

[5] Manning, W. (2010). CISM Certified Information Security Manager certification exam preparation course in a book for passing the CISM: The how to pass on your first try certification study guide. Brisbane, Australia: Emereo Pty Ltd.

что любая организация должна иметь свою собственную систему УИБ, внедрение которой является задачей специального комитета (совета директоров). Для последовательного внедрения УИБ в стране комитеты во всех организациях должны быть связаны друг с другом вышестоящим комитетом по УИБ или кибербезопасностью, который должен осуществлять общее управление. Кроме того, данная структура УИБ выступает в качестве инструмента для реализации управления информационной безопасностью, а также обеспечивает эффективность всего процесса в соответствии с целями и задачами бизнеса. Таким образом, предложенная структура УИБ составляет реальную программу безопасности, которая может быть применена к любой частной и государственной организации.

Список литературы

Al Neaimi, A., Ranginya, T., & Lutaaya, P. (2015). A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). *International Journal of Cyber-Security and Digital Forensics*, *4*(1), 290–301. https://doi.org/10.17781/p001502

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges AND CRITICAL SUCCESS FACTORS: Systematic review. *Computers & Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Bendovschi, A. (2015). Cyber-attacks – trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Bettwy, G., Beevers, M., & Williams, M. (2016). *CISM Review Manual Certified Information Security manager*. Rolling Meadows, Ill: ISACA.

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for Information Security Governance and Management. *IT Professional*, *18*(2), 22–30. https://doi.org/10.1109/mitp.2016.27

Carr, M., & Tanczer, L. M. (2018). UK cybersecurity industrial policy: An analysis of drivers, market failures and interventions. *Journal of Cyber Policy*, *3*(3), 430–444. https://doi.org/10.1080/23738871.2018.1550523

Corriss, L. (2010). Information security governance. *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies* (pp. 35–41). https://doi.org/10.1145/1920320.1920326

Creemers, R. (2023). Cybersecurity law and regulation in China: Securing the smart state. *China Law and Society Review*, *6*(2), 111–145. https://doi.org/10.1163/25427466-06020001

Fazlida, M. R., & Said, J. (2015). Information security: Risk, governance and implementation setback. *Procedia Economics and Finance*, *28*, 243–248. https://doi.org/10.1016/s2212-5671(15)01106-5

Hadi, M. A., Abdulredha, M. N., & Hasan, E. (2023). Introduction to ChatGPT: A new revolution of artificial intelligence with machine learning algorithms and cybersecurity. *Science Archives*, *04*(04), 276–285. https://doi.org/10.47587/sa.2023.4406

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126–129. https://doi.org/10.1145/1435417.1435446

Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers & Security*, *22*(7), 580–584. https://doi.org/10.1016/s0167-4048(03)00705-3

Nicho, M. (2018). A process model for implementing Information Systems Security governance. *Information & Computer Security*, *26*(1), 10–38. https://doi.org/10.1108/ics-07-2016-0061

Ohki, E., Harada, Y., Kawaguchi, Sh., Shiozaki, T., & Kagaya, T. (2009). Information security governance framework. *Proceedings of the first ACM workshop on Information security governance* (pp. 1–6). https://doi.org/10.1145/1655168.1655170

Priyadarshini, I., & Cotton, C. (2022). Cyber laws in the United States. *Cybersecurity (*pp. 157–237). https://doi.org/10.1201/9781003187127-6

Rao, U. H., & Nayak, U. (2014). History of computer security. *The InfoSec Handbook* (pp. 13–25). https://doi.org/10.1007/978-1-4302-6383-8_2

Rastogi, R., & von Solms, R. (2005). Information security governance – a re-definition. *Security Management, Integrity, and Internal Control in Information Systems* (pp. 223–236). https://doi.org/10.1007/0-387-31167-x_14

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*, *58*, 44–57. https://doi.org/10.1016/j.infsof.2014.10.003

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90–110. https://doi.org/10.1016/j.cose.2014.03.004

Shingarev, A., & Kazakova, A. (2021). The Russian Federation's approach to Cybersecurity. *The Oxford Handbook of Cyber Security* (pp. 672–684). https://doi.org/10.1093/oxfordhb/9780198800682.013.44

Singh, H. P., & Alshammari, T. S. (2020). An institutional theory perspective on developing a cyber security legal framework: A case of Saudi Arabia. *Beijing Law Review*, *11*(03), 637–650. https://doi.org/10.4236/blr.2020.113039

Tan, T. C., Ruighaver, A. B., & Ahmad, A. (2010). Information security governance: When compliance becomes more important than security. *Security and Privacy – Silver Linings in the Cloud* (pp. 55–67). https://doi.org/10.1007/978-3-642-15257-3_6

Ula, M., Ula, M., & Fuadi, W. (2017). A method for Evaluating Information Security Governance (ISG) components in banking environment. *Journal of Physics: Conference Series*, *812*, 012031. https://doi.org/10.1088/1742-6596/812/1/012031

Von Solms, S. H., & von Solms, R. (2010). *Information security governance*. New York, United States: Springer.

Von Solms, R., Thomson, K.-L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. *Information Security for South Africa* (pp. 1–6). https://doi.org/10.1109/issa.2011.6027522

Wu, M., Aranovich, R., & Filkov, V. (2021). Evolution and differentiation of the cybersecurity communities in three social question and answer sites: A mixed-methods analysis. PLOS ONE, 16(12). https://doi.org/10.1371/journal.pone.0261954

Сведения об авторах

Хади Мусадак Ахмед – магистр наук (инженер систем управления), кафедра управления и системной инженерии, Технологический университет
Адрес: Аль-Вейда, г. Багдад, Ирак
E-mail: musadaq.ahmed@alshaab.edu.iq
ORCID ID: https://orcid.org/0000-0002-3884-495X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57117413800
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JZT-4113-2024
Google Scholar ID: https://scholar.google.com/citations?user=wcrA7n8AAAAJ

Абдулредха Мохаммед Наджм – магистр компьютерных наук, кафедра компьютерных наук, Багдадский университет
Адрес: Аль-Джадрийя, г. Багдад, Ирак
E-mail: mohammed.najm.422@gmail.com
ORCID ID: https://orcid.org/0009-0007-8441-3505
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57226709471
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KIJ-3538-2024
Google Scholar ID: https://scholar.google.ru/citations?user=-oXQXKEAAAAJ

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.61 / Правовое регулирование информационной безопасности
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 16 апреля 2024 г.
Дата одобрения после рецензирования – 4 мая 2024 г.
Дата принятия к опубликованию – 25 марта 2025 г.
Дата онлайн-размещения – 30 марта 2025 г.

Research article
UDC 34:004:34.05:004.056.5
EDN: https://elibrary.ru/xujvtm
DOI: https://doi.org/10.21202/jdtl.2025.6

Universal Information Security Governance System: Organizational and Legal Principles

Musadaq Ahmed Hadi ✉
University of Technology, Baghdad, Iraq

Mohammed Najm Abdulredha
University of Baghdad, Baghdad, Iraq

Keywords

cybersecurity,
digital technologies,
information protection,
information security governance,
information security,
information technologies,
law,
legal regulation,
legislation,
organizational structure

Abstract

Objective: to develop universal organizational and legal principles for building an information security governance system that will allow each organization to create its own effective information security governance system, taking into account its unique business goals and tasks.

Methods: the research integrates the key elements of information security governance, such as vision, strategy, goals, policies, standards, processes, and matrices. Vision and goals set the direction of an organization's development; policies and standards provide a conceptual framework for information protection; processes allow for systematic achievement of objectives; and matrices provide tools for evaluating and monitoring the entire structure. The proposed principles are consistent with international standards, regulatory requirements, and best practices in the field of information security.

Results: the research showed that the developed information security governance system allows for a clear distribution of roles and responsibilities among the employees, ensuring effective implementation of the governance system. The authors also analyzed the existing principles of information security, integrating them into a security strategy that meets the corporate goals. The proposed universal system complies with regulatory legal requirements and can be adapted for organizations of any scale and profile.

✉ Corresponding author

Scientific novelty: the paper represents a practical approach to the implementation of an information security governance system based on the authors' experience, international standards, control systems and legal acts. Unlike existing approaches, the proposed system is flexible and can be adapted to any organization, which makes it a universal tool for information security governance.

Practical significance: the research provides a structured approach to creating a universal information security governance system that can be used by organizations lacking knowledge and resources to implement such initiatives. The authors propose a general structure that can be adapted depending on the organization's assets, the employees' training and awareness of information security issues. This makes the paper a valuable resource for professionals seeking to increase information security in their organizations.

For citation

Hadi, M. A., & Abdulredha, M. N. (2025). Universal Information Security Governance System: Organizational and Legal Principles. *Journal of Digital Technologies and Law, 3*(1), 125–142. https://doi.org/10.21202/jdtl.2025.6

References

Al Neaimi, A., Ranginya, T., & Lutaaya, P. (2015). A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). *International Journal of Cyber-Security and Digital Forensics*, *4*(1), 290–301. https://doi.org/10.17781/p001502

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges AND CRITICAL SUCCESS FACTORS: Systematic review. *Computers & Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Bendovschi, A. (2015). Cyber-attacks – trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Bettwy, G., Beevers, M., & Williams, M. (2016). *CISM Review Manual Certified Information Security manager*. Rolling Meadows, Ill: ISACA.

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for Information Security Governance and Management. *IT Professional*, *18*(2), 22–30. https://doi.org/10.1109/mitp.2016.27

Carr, M., & Tanczer, L. M. (2018). UK cybersecurity industrial policy: An analysis of drivers, market failures and interventions. *Journal of Cyber Policy*, *3*(3), 430–444. https://doi.org/10.1080/23738871.2018.1550523

Corriss, L. (2010). Information security governance. *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies* (pp. 35–41). https://doi.org/10.1145/1920320.1920326

Creemers, R. (2023). Cybersecurity law and regulation in China: Securing the smart state. *China Law and Society Review*, *6*(2), 111–145. https://doi.org/10.1163/25427466-06020001

Fazlida, M. R., & Said, J. (2015). Information security: Risk, governance and implementation setback. *Procedia Economics and Finance*, *28*, 243–248. https://doi.org/10.1016/s2212-5671(15)01106-5

Hadi, M. A., Abdulredha, M. N., & Hasan, E. (2023). Introduction to ChatGPT: A new revolution of artificial intelligence with machine learning algorithms and cybersecurity. *Science Archives*, *04*(04), 276–285. https://doi.org/10.47587/sa.2023.4406

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126–129. https://doi.org/10.1145/1435417.1435446

Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers & Security*, *22*(7), 580–584. https://doi.org/10.1016/s0167-4048(03)00705-3

Nicho, M. (2018). A process model for implementing Information Systems Security governance. *Information & Computer Security*, *26*(1), 10–38. https://doi.org/10.1108/ics-07-2016-0061

Ohki, E., Harada, Y., Kawaguchi, Sh., Shiozaki, T., & Kagaya, T. (2009). Information security governance framework. *Proceedings of the first ACM workshop on Information security governance* (pp. 1–6). https://doi.org/10.1145/1655168.1655170

Priyadarshini, I., & Cotton, C. (2022). Cyber laws in the United States. *Cybersecurity (*pp. 157–237). https://doi.org/10.1201/9781003187127-6

Rao, U. H., & Nayak, U. (2014). History of computer security. *The InfoSec Handbook* (pp. 13–25). https://doi.org/10.1007/978-1-4302-6383-8_2

Rastogi, R., & von Solms, R. (2005). Information security governance – a re-definition. *Security Management, Integrity, and Internal Control in Information Systems* (pp. 223–236). https://doi.org/10.1007/0-387-31167-x_14

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*, *58*, 44–57. https://doi.org/10.1016/j.infsof.2014.10.003

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90–110. https://doi.org/10.1016/j.cose.2014.03.004

Shingarev, A., & Kazakova, A. (2021). The Russian Federation's approach to Cybersecurity. *The Oxford Handbook of Cyber Security* (pp. 672–684). https://doi.org/10.1093/oxfordhb/9780198800682.013.44

Singh, H. P., & Alshammari, T. S. (2020). An institutional theory perspective on developing a cyber security legal framework: A case of Saudi Arabia. *Beijing Law Review*, *11*(03), 637–650. https://doi.org/10.4236/blr.2020.113039

Tan, T. C., Ruighaver, A. B., & Ahmad, A. (2010). Information security governance: When compliance becomes more important than security. *Security and Privacy – Silver Linings in the Cloud* (pp. 55–67). https://doi.org/10.1007/978-3-642-15257-3_6

Ula, M., Ula, M., & Fuadi, W. (2017). A method for Evaluating Information Security Governance (ISG) components in banking environment. *Journal of Physics: Conference Series*, *812*, 012031. https://doi.org/10.1088/1742-6596/812/1/012031

Von Solms, S. H., & von Solms, R. (2010). *Information security governance*. New York, United States: Springer.

Von Solms, R., Thomson, K.-L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. *Information Security for South Africa* (pp. 1–6). https://doi.org/10.1109/issa.2011.6027522

Wu, M., Aranovich, R., & Filkov, V. (2021). Evolution and differentiation of the cybersecurity communities in three social question and answer sites: A mixed-methods analysis. PLOS ONE, 16(12). https://doi.org/10.1371/journal.pone.0261954

Authors information

Musadaq Ahmed Hadi – MSc. (Control Engineer), Control and Systems Engineering Department, University of Technology
Address: Al-Wehda, Baghdad, Iraq
E-mail: musadaq.ahmed@alshaab.edu.iq
ORCID ID: https://orcid.org/0000-0002-3884-495X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57117413800
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JZT-4113-2024
Google Scholar ID: https://scholar.google.com/citations?user=wcrA7n8AAAAJ

Mohammed Najm Abdulredha – MSc. (Computer Science), Department of Computer Science, University of Baghdad
Address: Al-Jadriya, Baghdad, Iraq
E-mail: mohammed.najm.422@gmail.com
ORCID ID: https://orcid.org/0009-0007-8441-3505
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57226709471
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KIJ-3538-2024
Google Scholar ID: https://scholar.google.ru/citations?user=-oXQXKEAAAAJ

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declare no conflict of interest.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – April 16, 2025
Date of approval – May 4, 2025
Date of acceptance – March 25, 2025
Date of online placement – March 30, 2025