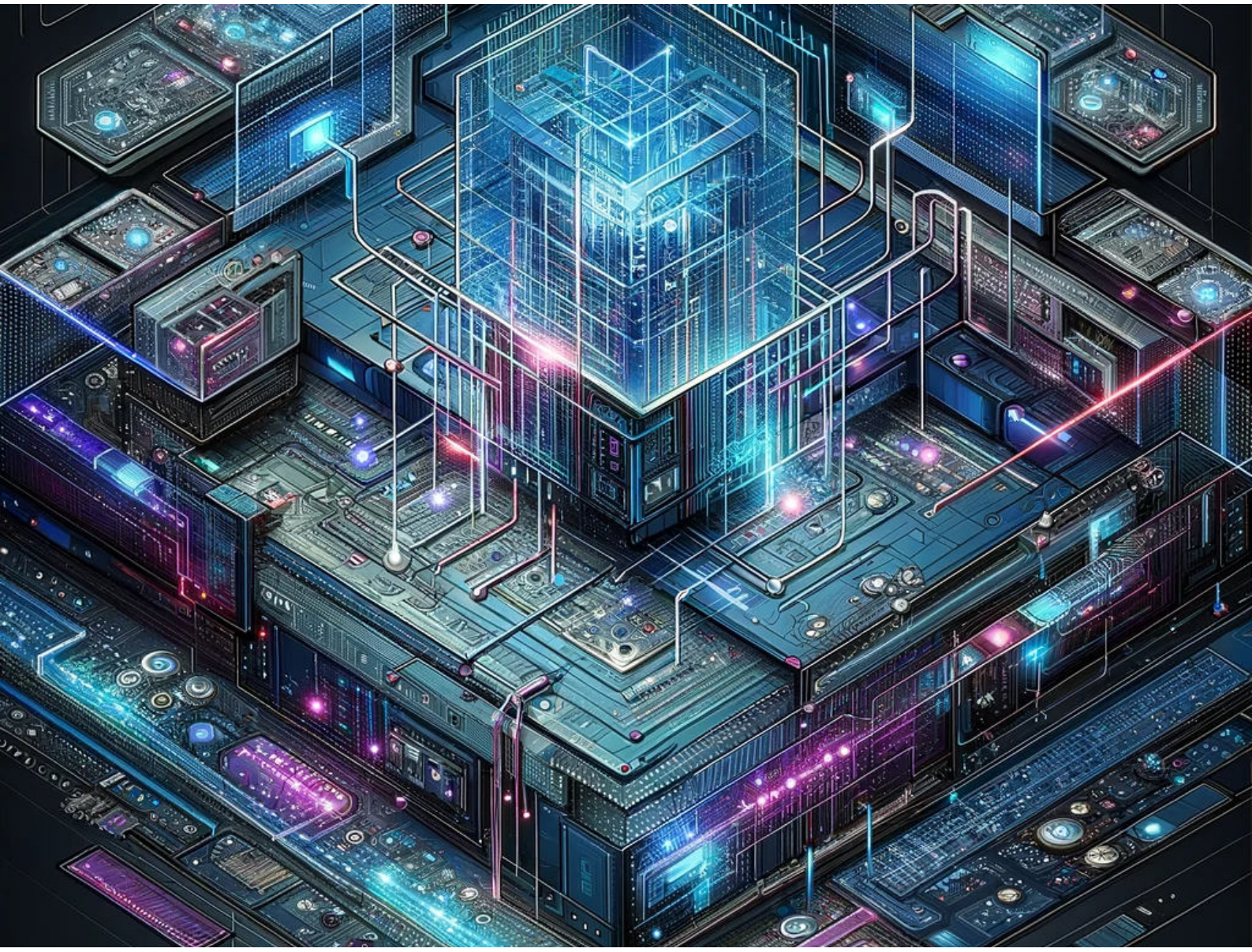
ACSH
Partnership for Excellence

Ministry of the Interior and Safety
Republic of Korea

NIA
NATIONAL INFORMATION SOCIETY AGENCY

UNDP

Рамочные стандарты для **цифровой** трансформации



Программа развития Организации Объединенных Наций
Астанинский хаб государственной службы
Астана 2023

Данная публикация является одним из результатов работы проекта «Укрепление потенциала для развития инноваций в государственном управлении и цифровизации государственных услуг», финансируемого Правительством Республики Корея и реализуемого Программой развития ООН (ПРООН) в Казахстане и Астанинским хабом государственной службы (ACSH) в тесном сотрудничестве с Министерством внутренних дел и безопасности (MOIS) и Национальным агентством по вопросам по вопросам информационного общества (NIA) Республики Корея.

Публикация предназначена для политиков, практиков, экспертов, ученых, студентов и всех, кто интересуется вопросами, связанными с открытыми государственными данными.

Для цитирования:

ACSH (2023). Рамочные стандарты для цифровой трансформации. Астана, Казахстан: Астанинский хаб государственной службы.

© ПРООН 2023
© Астанинский хаб государственной службы 2023

Взгляды и мнения, выраженные в настоящем документе, не обязательно отражают точку зрения Астанинского хаба государственной службы и/или ПРООН. Фотокопии и воспроизведение выдержек из текста разрешаются при указании соответствующих ссылок.

Вступительное слово

Стремительное и масштабное внедрение цифровых технологий и их далеко идущее всепроникающее воздействие на людей диктуют необходимость разработки стандартов по управлению цифровой трансформацией. Определенно необходим набор минимальных общих принципов и руководящих указаний для определения и стандартизации таких аспектов, как безопасность, надежность, эффективность, совместимость и доверие к цифровым системам и средам (ЮНИДО, 2021).

Стандарты играют решающую роль в формировании процесса цифровой трансформации, поскольку они обеспечивают общую основу для применения цифровых технологий. Они также дополняют нормативные акты и законы, способствуя управлению цифровой трансформацией. Принятие стандартов способствует совместимости и интероперабельности услуг, продуктов и процессов, гарантируя при этом минимально необходимый уровень качества и безопасности. Более того, стандарты могут служить ускорителями перемен, поскольку они способствуют инновациям и могут обеспечить успешное масштабирование цифровых решений для решения общих проблем.

Данная публикация была подготовлена в рамках проекта, реализуемого совместными усилиями Министерства внутренних дел и безопасности (MOIS) и Национального агентства по развитию информационного общества (NIA) Республики Корея, Программы развития Организации Объединенных Наций (ПРООН) в Казахстане и Астанинского хаба государственной службы (ACSH). Она содержит подробное описание нескольких рамочных стандартов, используемых во всем мире. Публикация охватывает такие области, как эффективное использование информационных технологий, кибербезопасность, защита конфиденциальности данных, облачные вычисления, инфраструктура и т.д., и может способствовать цифровой трансформации государственного сектора стран-участниц.

Мы надеемся, что эта публикация будет полезна в процессе усилению цифровизации в деятельности государственного сектора и улучшению оказания государственных услуг. Публикация внесет значимый вклад в прогресс и успех стран-участниц в постоянно меняющемся цифровом ландшафте, поскольку здесь содержится ценная информация и продвигаются самые высокие стандарты цифровой трансформации,

Мы искренне надеемся, что содержание данной публикации окажется для вас информативным и полезным. Ее основная цель – внести вклад в приобретение знаний и опыта для активизации усилий и действий стран-участниц по созданию надежных цифровых систем.

Сух, Бо Рам
Заместитель министра
по цифровому правительству
Министерство внутренних дел и безопасности
Республика Корея

Алихан Байменов
Председатель
Управляющего комитета
Астанинского хаба
государственной службы

Выражение благодарности

Данная публикация является одним из результатов работы проекта «Укрепление потенциала для развития инноваций в государственном управлении и цифровизации государственных услуг», совместно реализуемого Программой развития Организации Объединенных Наций (ПРООН) в Казахстане и Астанинским хабом государственной службы (ACSH), с одной стороны, и Министерством внутренних дел и безопасности (МВДиБ) и Национальным агентством по развитию информационного общества (NIA) Республики Корея, с другой стороны.

Проект направлен на укрепление потенциала государственных служащих и специалистов-практиков, участвующих во внедрении инноваций в системе государственного управления и цифровизации государственных услуг в семи странах Центральной Азии (Казахстан, Кыргызская Республика, Таджикистан и Узбекистан) и Кавказа (Армении, Азербайджана и Грузии). Проект рассчитан на три года (2021-2023 гг.) и включает семинары по укреплению потенциала, а также подготовку публикаций.

Отдельная благодарность выражается команде исследований и управления знаниями ACSH за их труд и время, вложенные в подготовку данной публикации.

Мы признательны Правительству Республики Корея за значительную финансовую поддержку и существенный вклад в содержательную часть этой работы.

О Министерстве внутренних дел и безопасности (MOIS)

Министерство внутренних дел и безопасности (MOIS) отвечает за общие вопросы Государственного совета, публикацию законов, подзаконных актов и международных договоров, организацию деятельности правительства и установленную численность государственных служащих, награды и знаки отличия, вопросы государственных инноваций, административной эффективности, цифрового правительства, защиту персональных данных, управления государственными зданиями и поддержку в проведении выборов и референдумов. Кроме того, MOIS активно содействует развитию автономии на местном уровне и децентрализации, поддерживая хозяйственную деятельность, финансы и налогообложение местных органов власти и выступая посредником в спорах между местными органами власти. Кроме того, MOIS отвечает за разработку, осуществление надзора и внесение изменений в политику, связанных с безопасностью и управлением стихийными бедствиями, такими как борьба с чрезвычайными ситуациями, защита граждан и предотвращение стихийных бедствий.

Имея такую миссию как руководство государственными инновациями в целях устойчивого будущего путем оказания более интегрированных и персонализированных услуг для граждан, содействия этичному и эффективному использованию цифровых технологий и укрепления государственно-частных партнерств, MOIS возглавляет процесс цифровой трансформации государственного сектора и сотрудничает со странами-партнерами в целях построения лучшего цифрового общества во всем мире.

Более подробная информация на сайте https://www.mois.go.kr/eng/sub/a02/aboutMinistry/screen.do.

Национальном агентстве по развитию информационного общества (NIA)

Национальное агентство по развитию информационного общества является государственной организацией, созданной в 1987 г. в соответствии с Рамочным законом о содействии информатизации (Статья 10), при Министерстве науки и ИКТ и Министерстве внутренних дел и безопасности Кореи. С момента своего создания оно играет ведущую роль в продвижении национальной информатизации и цифрового правительства Кореи. Агентство осуществляло управление важными политиками в области ИКТ и инфраструктурными проектами, включая Генеральный план национальной базовой информационной системы (1987 г.), создание сверхскоростной информационной сети (1995 г.), 11 инициатив и 31 задачу для электронного правительства (2001 и 2003 гг. соответственно), участвовало в принятии Закона о содействии предоставлению и использованию публичных данных (2013 г.), а также в разработке и продвижении стратегии 5G+ и национальной стратегии искусственного интеллекта (2019 г.).

С наступлением эпохи цифровой трансформации NIA работает над разработкой и использованием ключевых технологий ИКТ для внедрения стратегии DNA+ для успешного превращения Кореи в интегрированное информационное общество. «DNA+» означает данные, сеть, ИИ, а знак «+» символизирует упреждающие меры реагирования на различные проблемы, такие как цифровой разрыв между различными слоями общества и чрезмерная зависимость от различных устройств ИКТ. Его конечной целью является решение социальных проблем и открытие будущего для нации с помощью ИКТ.

Более подробная информация на сайте https://eng.nia.or.kr/site/nia_eng/04/10401000000002016093002.jsp.

О Программе развития ООН (ПРООН)

Программа развития ООН (ПРООН) — ведущая организация ООН, борющаяся за то, чтобы положить конец несправедливости, связанной с бедностью, неравенством и изменением климата. Работая с широкой сетью экспертов и партнеров в 170 странах, ПРООН помогает странам создавать комплексные, долгосрочные решения для людей и планеты.

Дополнительная информация на сайте www.undp.org.

Об Астанинском хабе государственной службы (ACSH)

Астанинский хаб государственной службы является флагманской инициативой правительства Казахстана и Программы развития ООН. ACSH является многосторонней институциональной платформой для непрерывного обмена знаниями и опытом в области развития государственной службы с целью поддержки правительств в регионе посредством развития партнерских отношений, наращивания потенциала и взаимного обучения, а также исследований, основанных на фактических данных.

Он был создан в 2013 году 5 международными организациями и 25 странами: сейчас в его состав входят 43 страны-участницы и более 90 организации. География участников простирается от Америки и Европы через СНГ, Кавказ и Центральную Азию до стран АСЕАН, демонстрируя, что партнерство для повышения качества государственной службы является постоянной и универсальной потребностью для всех стран.

Миссия ACSH заключается в содействии повышению эффективности государственной службы посредством поддержки усилий правительств стран-участниц в наращивании институционального и человеческого потенциала, таким образом, способствуя совершенствованию систем государственной службы в странах региона и за его пределами.

Более подробная информация на сайте www.astanacivilservicehub.org.

Оглавление

Вступительное слово I
Выражение благодарности II
О Министерстве внутренних дел и безопасности (MOIS) III
О Национальном агентстве по развитию информационного общества (NIA) IV
О Программе развития ООН (ПРООН) V
Об Астанинском хабе государственной службы (ACSH) VI
Оглавление V
Список рисунков XI
Список таблиц XI
Список вставок XII

Введение 1

I. Библиотека инфраструктуры информационных технологий (ITIL) 6
I.1. Введение 6
I.1.1 ITIL и его эволюция 6
I.1.2 Объяснение необходимости стандартизированных методов управления ИТ-услугами 7
I.2. Обзор 8
I.2.1 Ключевые концепции, принципы и процессы 8
I.2.2 Важность концепций и процессов: повышение качества предоставления и управления ИТ-услугами 10
I.2.3 Архитектура ITIL и подход жизненного цикла 10
I.2.4 Преимущества внедрения ITIL 11
I.3. Роли и обязанности в ITIL 12
I.3.1 Изучение различных ролей и обязанностей в рамках ITIL 12
I.3.2 Важность ясности ролей и подотчетности в управлении ИТ-услугами 13
I.4. Процесс внедрения 14
I.4.1 Шаги по принятию и внедрению ITIL 14
I.4.2 Проблемы и соображения по внедрению ITIL 15
I.4.3 Стратегии успешного внедрения 16
I.5. Практические примеры 16
I.6. Выводы 17
I.7. Краткое резюме 18
I.8. Список литературы 20

II. Архитектура взаимодействия электронного правительства (e-GIF) 21
II.1. Введение 21
II.2. Обзор Архитектуры взаимодействия электронного правительства (e-GIF) 22
II.2.1 Определение e-GIF 22
II.2.2. Структура e-GIF 23
II.2.2.1 Архитектура e-GIF 23
II.2.2.2 e-GMS 24
II.2.2.3 Каталог государственных стандартов данных (GDS) 24
II.2.2.4 XML-схемы 24
II.2.2.5 Каталог технических стандартов 25

II.2.2.6 Техническая политика 25
II.2.2.7 Поддержка внедрения и т.д. 26
II.2.3 Статус различных рамочных стандартов по интероперабельности 28
II.2.3. 1 Европейский свод требований по совместимости 29
II.2.3.2 X-Road (X-tee) 30
II.2.3.3 Архитектура предприятия (EA) 31
II.2.3.4 Стандартная структура электронного правительства 31
II.2.4. Международные исследования (ООН, ВБ, ОЭСР) и стандарты совместимости 31
II.2.4.1 ООН (EGDI) 32
II.2.4.2 Всемирный банк (GTMI) 32
II.2.4. 3 ОЭСР (DGI) 33
II.3 Сравнение различных стандартов e-GIF 34
II.4 Объяснение различных рамок обеспечения совместимости 37
II.4.1 Европейский свод требований по совместимости (EIF) 37
II.4.2 X-Road (X-tee) 38
II.4.3 Рамочная структура архитектуры федерального предприятия (FEAF) 41
II.4.3.1 Консолидированная эталонная модель 41
II.4.3.2 Методология совместного планирования 42
II.4.3. 3 артефакта 43
II.4.4.5 Стандартная структура электронного правительства 45
II.5 Заключение 48
II.5.1 Управление 48
II.5.2 Выбор подходящей модели e-GIF 48
II.5.3 Выбор подходящей технологии 48
II.6 Список литературы 49
II.7 Приложение: Содержание Каталога технических стандартов (TSC, версия 6.2) 50

III. Методика описания архитектуры, разработанная Open Group (TOGAF) и ЗАДАЧИ УПРАВЛЕНИЯ информационных И СМЕЖНЫХ технологий (COBIT) 51
III.1. Введение 51
III.2. Обзор методологий систем хранения и обмена данными 52
III.2.1 TOGAF 52
III.2.1.1 Введение в TOGAF 52
III.2.1.2 Ключевые компоненты TOGAF 54
III.2.1.3 Процесс внедрения TOGAF 55
III.2.2 COBIT 57
III.2.2.1 Введение в COBIT 57
III.2.2.3 Ключевые компоненты COBIT 58
III.2.2.4 Процесс внедрения COBIT 59
III.2.3 Внедрение структуры общеорганизационной архитектуры в Южной Корее 60
III.2.3.1 Ключевые компоненты структуры архитектуры предприятия 61
III.2.3.2 Процесс реализации EA 62
III.3 Сравнение TOGAF, COBIT, GEAP 66
III.4. Презентация вариантов использования и передовой практики (примеры Кореи) 70

IV. ЭТАЛОННАЯ АРХИТЕКТУРА ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ 76
IV.1. Введение 76
IV.2. Ключевые принципы облачной эталонной архитектуры 76
IV.3. Принципы создания эталонной облачной архитектуры 76
IV.4. Компоненты архитектуры исходя из видов облачных сервисов 77
IV.4.1 IaaS (Инфраструктура как услуга) 78
IV.4.2 PaaS (платформа как услуга) 79
IV.4.3 SaaS (Программное обеспечение как услуга) 80
IV.5. Модели архитектуры исходя из типов развертывания облачных сервисов 81
IV.5.1 Публичное/частное облако 81
IV. 5.2 Гибридное облако 82
IV.5.3 Мультиоблако 83
IV.5.4 Периферийное облако 84
IV.5.5 Микросервисная архитектура 85
IV.5.6 Бессерверная архитектура 86
IV.6. Детальные технические компоненты облачной архитектуры 87
IV.6.1 Облачная безопасность и управление авторизацией 87
IV.6.2 Надежность и доступность 88
IV.6.3 Оптимизация производительности 89
IV.6.4 Облачная сеть 90
IV.6.5 Управление облачными данными 91
IV.6.6 Облачная автоматизация 92
IV.6.7 Управление и мониторинг облака 93
IV.7. Рекомендации по внедрению облачных вычислений для государственного управления 93
IV.7.1 Миграция на IaaS 94
IV.7.2 Миграция с использованием PaaS 95
IV.7.3 Переход на SaaS 96
IV.7.4 Миграция в гибридное облако 96
IV.8. Практические примеры и результаты внедрения облачных технологий в государственных учреждениях 97
IV.8.1 Внедрение IaaS 97
IV.8.2 Внедрение PaaS/SaaS 98
IV.9. Сравнение с другими облачными платформами 99
IV.9.1 Облачная платформа НИСТ 99
IV.9.2 Эталонная облачная архитектура ISO/IEC 17789 99
IV.9.3 Сравнение с другими архитектурами: преимущества и ожидаемые эффекты 101
IV.10. Список литературы 103

V. ОБЩИЙ РЕГЛАМЕНТ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ (GDPR) В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ 104
V.1. Введение 104
V.2. Важность GDPR в государственном управлении 105
V.3. Обзор GDPR и его основных положений 106
V.4. Историческое развитие законодательства в области защиты данных 108
V.5. Основные принципы GDPR 109
V.6. Сертификация 110
V.6.1 GDPR-CARPA 111

V.6.2 Euro privacy....112
V.6.3. Процесс сертификации....113
V.7. Влияние GDPR на государственное управление....114
V.8. Практические шаги по внедрению....116
V.9. Трудности при внедрении GDPR в государственном управлении....117
V.10. Примеры из практики: примеры внедрения GDPR в государственном управлении....118
V.10.1 Германия - Стандартная модель защиты данных....119
V.10.2 Нидерланды – Стандарты информационной безопасности и защиты данных для фундаментального образования....119
V.10.3 Франция – Образовательный модуль для местных исполнительных органов....120
V.11. Заключение....121
V.12. Список литературы....123

VI. ISO/IEC 27001:2022....124
VI.1. Введение и обзор стандарта ISO/IEC 27001:2022....124
VI.2. Принципы и задачи....124
VI.3. Детальный анализ технических спецификаций и требований....126
VI.4. Основной этап создания СУИБ....130
Этап 1: Контекстный анализ....130
Этап 2: Анализ и оценка рисков....130
Этап 3: Обработка риска в соответствии с результатами оценки риска....130
Этап 4: Меры контроля информационной безопасности (цели и меры контроля Приложения А)....130
Этап 5: Функционирование (функционирование и управление в соответствии с результатами оценки рисков)....130
Этап 6: Мониторинг (внутренний аудит и мероприятия в рамках анализа со стороны руководства)....131
Этап 7: Последующее управление (пост-сертификационный аудит один раз в год)..131
VI.5. Обзор практических примеров использования....131
VI.5.1 Конкретный реальный пример успешного внедрения ISO 27001....133
VI.6. Преимущества внедрения стандарта ISO 27001....134
VI.7. Ограничения и недостатки системы ISO 27001....135
VI.8. Рекомендации по эффективному применению и внедрению стандарта ISO 27001....135

VII. СТАНДАРТ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ - ISO 29100....136
VII.1.1 Важность кибербезопасности и конфиденциальности в современном цифровом пространстве....136
VII.2. Функции системы кибербезопасности и конфиденциальности для организации и страны....138
VII.3. Общие сведения и контекст....139
VII.3.1 Представление концепции кибербезопасности и конфиденциальности; их значение в современном цифровом мире....139
VII.3.2 Обзор вызовов и угроз, связанных с кибербезопасностью и конфиденциальностью....140

VII.4. Обсуждение необходимости разработки систем кибербезопасности и конфиденциальности для поддержки организаций в их деятельности по обеспечению кибербезопасности и конфиденциальности....142
VII.5. Обзор системы кибербезопасности и конфиденциальности....144
VII.5.1 Подробное объяснение системы кибербезопасности и конфиденциальности....144
VII.5.2 Рамочный стандарт обеспечения кибербезопасности....146
2) ISO 27001 72....147
VII.5.3 Рамочный стандарт обеспечения конфиденциальности....148
1) Стандарт обеспечения конфиденциальности НИСТ....148
2) ISO 29100....149
VII.6. Сравнение различных стандартов кибербезопасности и конфиденциальности....151
VII.7. Практические примеры....151
VII.7.1. Реальные примеры организаций, успешно внедривших системы обеспечения кибербезопасности и конфиденциальности....151
1) Cisco Systems....151
2) Microsoft....152
3) Округ Арлингтон, штат Вирджиния....155
VII.8. Вызовы и барьеры, возникшие при принятии и внедрении систем....155
VII.9. Будущие тенденции и новые системы....156
VII.9.1 Новые тенденции и разработки в области кибербезопасности и конфиденциальности....156
VII.9.2 Ознакомление с другими или готовящимися выпуску системами обеспечения кибербезопасности и конфиденциальности, которые могут оказать влияние на цифровую среду....157
VII.10. Заключение....159

Обсуждение....162
Аббревиатуры и сокращения....167

Список рисунков

Рис. 1: Архитектура e-GIF 23
Рис. 2: Пересмотренная концептуальная модель EIF 38
Рис. 3: Архитектура X-Road 39
Рис. 4. Экосистема X-Road 41
Рис. 5. Консолидированная эталонная модель 42
Рис. 6. Методология совместного планирования 43
Рис. 7: Артефакты EA 44
Рис. 8: Стандартизация структуры электронного правительства 45
Рис. 9: Структура стандартной структуры электронного правительства 47
Рис. 10: Структура TOGAF 54
Рис. 11: Матрица интероперабельности в TOGAF 56
Рис. 12. Общая архитектура облака 77
Рис. 13. Модели архитектуры исходя из типов развертывания облачных сервисов 81
Рис. 14. Детальные технические компоненты облачной архитектуры 88
Рис. 15: Критерии и характеристики определения типа облака 95
Рис. 16. Эффекты внедрения IaaS государственными учреждениями 97
Рис. 17: Эффект от внедрения SaaS/PaaS государственными учреждениями 98
Рис. 18. Эталонная архитектура облачных вычислений НИСТ 99
Рис. 19. Эталонная архитектура облачных вычислений в стандарте ISO/IEC 17789 101
Рис. 20: Критерии подотчетности 112
Рис. 21: Основные критерии GDPR 113
Рис. 22: Процесс сертификации 114
Рис. 23: Куб стандартной модели данных (англ. SDM) 119

Список таблиц

Таблица 1. Основные причины стандартизации практики управления ИТ-услугами 9
Таблица 2: Пример таблицы TSC (спецификации межсетевого взаимодействия) 23
Таблица 3. Краткое описание содержания разделов 3-6 e-GIF 23
Таблица 4: Текущая политика и законы в отношении данных в ведущих странах 28
Таблица 5: Исследование ВБ GTMI: Основная государственная система, 1_3. GIF 33
Таблица 6: Сравнение политики в области интероперабельности 35
Таблица 7: Основной документ 44
Таблица 8: Архитектура стандартной структуры электронного правительства 47
Таблица 9: Ключевые компоненты структуры архитектуры предприятия 61
Таблица 10: Ключевые компоненты процесса управления EA 63
Таблица 11: Особенности, преимущества и недостатки различных платформ 64
Таблица 12: Сравнение TOGAF, COBIT, GEAP 68

Список вставок

Вставка 1: Основные документы, относящиеся к e-GMS 24
Вставка 2: Меню данных GDS 24
Вставка 3: Межсетевые соединения (Пример технической политики) 25
Вставка 4: Пример рекомендации 38
Вставка 5: Особенности X-Road 39
Вставка 6: Видение, цели и стратегии Стандартной структуры электронного правительства 46
Вставка 7: Стандартный документ TOGAF 53

Введение

В эпоху непрерывного развития цифровых технологий потребность в стандартах в сфере управления цифровой трансформацией становится все более очевидной. Глубокое и обширное влияние этих технологий на людей, организации и общества подчеркивает настоятельную необходимость создания общего комплекса принципов и руководств для обеспечения бесперебойной и безопасной работы цифрового ландшафта. Эти стандарты необходимы для формирования пути продвижения на цифровом фронте, определяя такие параметры, как безопасность, надежность, эффективность, совместимость и доверие к цифровым системам и средам. Устанавливая общие минимальные стандарты, мы создаем основу, на которой цифровой мир может развиваться, процветать и в конечном итоге приносить пользу человечеству.

Важность этих стандартов невозможно переоценить. Они обеспечивают общие рамки, которые повышают совместимость и интероперабельность цифровых услуг, продуктов и процессов. Это, в свою очередь, позволяет гарантировать минимально необходимый уровень качества и безопасности, тем самым создавая ощущение единообразия в цифровой сфере. Более того, стандарты играют важную роль в содействии инновациям, выступая катализатором позитивных изменений в технологическом ландшафте. Придерживаясь этих стандартов, цифровые решения можно масштабировать для эффективного решения общих проблем, обеспечивая доступность преимуществ цифровой трансформации для всех.

Последствия установления таких стандартов выходят далеко за рамки цифровой сферы. За счет обеспечения доступа эти стандарты могут сломать пространственные и социальные барьеры, способствуя созданию более инклюзивного и взаимосвязанного мира. Они открывают двери для новых форм занятости и предпринимательства, давая людям возможность пользоваться огромными возможностями, предоставляемыми цифровой эпохой. Однако в этой трансформации также таится угроза вытеснения автоматизацией и робототехникой традиционных рабочих мест, что подчеркивает необходимость тщательного и внимательного управления цифровой трансформацией. В этом сложном взаимодействии между технологиями и обществом стандартизация становится путеводным компасом, помогая нам двигаться к будущему, в котором будут реализованы преимущества цифровых инноваций, сводя при этом к минимуму потенциальные сбои и обеспечивая благополучие для всех.

Цифровые технологии с их трансформационным потенциалом открывают уникальный путь для достижения и продвижения Целей устойчивого развития (ЦУР) Организации Объединенных Наций, в частности ЦУР 16 и ЦУР 17. ЦУР 16 направлена на создание мирных, справедливых и инклюзивных обществ путем равного распределения выгод, обеспечиваемых цифровыми технологиями. Рамочные стандарты в области управления цифровой трансформацией играют важную роль в достижении этой цели. Обеспечивая соответствие цифровых систем и сред принципам справедливости, безопасности и доверия, эти стандарты могут помочь преодолеть цифровой разрыв, гарантируя доступность всем преимуществ технологического прогресса. Благодаря установлению общих минимальных стандартов маргинализированные сообщества смогут более полно участвовать в жизни общества в эпоху цифровых технологий, способствуя тем самым социальной интеграции и справедливости.

Более того, транснациональный характер многих прорывных цифровых технологий требует скоординированных международных усилий по созданию эффективных правил и политики, соответствующих принципам ЦУР 17. Стандартизация в управлении цифровой трансформацией играет ключевую роль в развитии глобального сотрудничества и партнерства. Поскольку разные страны и регионы осуществляют цифровую трансформацию, рамочные стандарты обеспечивают общий язык и определенные ожидания, которые способствуют международному консенсусу по вопросам регулирования. Эти стандарты создают основу для гармонизации политики и регулирования между странами, обеспечивая бесперебойность трансграничных потоков данных, торговли и сотрудничества. В стремлении к устойчивому развитию, особенно в таких областях, как изменение климата, здравоохранение и сокращение бедности, международное сотрудничество, подкрепленное стандартами цифровых технологий, становится основой успеха, позволяя странам эффективно работать сообща для достижения общих целей ЦУР.

По сути, установление стандартов цифровых технологий не только служит мостом для обеспечения справедливого распределения выгод в соответствии с ЦУР 16, но также способствует международному сотрудничеству и достижению консенсуса, являющимся важным элементом в продвижении трансформационной повестки дня ЦУР, в частности ЦУР 17. Эти стандарты обеспечивают необходимую основу, на которой может быть построен более мирный, справедливый, инклюзивный и устойчивый мир в эпоху цифровых технологий, что в конечном итоге приведет нас к более процветающему и гармоничному будущему для всех.

Взаимосвязь между стандартами, правилами и политикой образует замкнутую и взаимозависимую экосистему, лежащую в основе концепции надлежащего управления в эпоху цифровых технологий. Стандарты обеспечивают основополагающую основу, на которой строятся надежные правила и политика. Надлежащее управление гарантирует, что цифровая трансформация способствует повышению благосостояния общества, одновременно снижая риски и дисбалансы.

Стандарты предлагают общие принципы и рекомендации, служащие основой для создания эффективных правил. Регулирующие органы и политики используют эти стандарты для разработки законов, которые соответствуют цифровому ландшафту, обеспечивая последовательность и предсказуемость.

В свою очередь, хорошо продуманные правила и политика укрепляют стандарты, закрепляя их в законодательстве, усиливая степень их соблюдения и стимулируя инновации. Они также способствуют прозрачности, подотчетности и справедливости, являющимся жизненно важными компонентами надлежащего управления. Эта двусторонняя связь способствует созданию среды, в которой цифровая трансформация происходит в этических и безопасных рамках, способствуя справедливому, инклюзивному и процветающему будущему для всех.

В сфере цифровой трансформации разработка и внедрение стандартов регулируются несколькими ключевыми принципами, каждый из которых способствует достижению главной цели надлежащего управления. Эти принципы являются фундаментальными элементами, на которых может быть построен цифровой ландшафт на благо всех.

1. ***Надежность:*** в основе цифрового взаимодействия лежит доверие. Стандарты должны обеспечивать надежность цифровых систем, гарантируя пользователям безопасность, надежность и прозрачность их данных и транзакций.
2. ***Инклюзивность:*** в рамках цифровой трансформации никто не должен остаться без внимания. Стандарты должны быть разработаны таким образом, чтобы способствовать инклюзивности, делая технологии доступными и полезными для всех людей и сообществ, независимо от их обстоятельств.
3. ***Устойчивость:*** по мере расширения цифрового мира его влияние на окружающую среду становится все более очевидным. Стандарты должны уделять первоочередное внимание устойчивому развитию, поощряя экологически чистые методы, ответственное использование ресурсов и энергоэффективность.
4. ***Функциональная совместимость (интероперабельность):*** В мире разнообразных цифровых систем функциональная совместимость имеет ключевое значение. Стандарты должны обеспечивать беспрепятственную совместную работу различных технологий, улучшая пользовательский опыт и продвигая инновации.
5. ***Безопасность и защищенность:*** Киберугрозы присутствуют везде. Стандарты должны уделять приоритетное внимание безопасности и защищенности, обеспечивая надежную основу для защиты систем и данных, а также снижения рисков и уязвимостей.
6. ***Конфиденциальность данных:*** Персональные данные являются ценным активом. Стандарты должны обеспечивать конфиденциальность данных, защищать права людей и укреплять доверие к цифровому взаимодействию.
7. ***Международное сотрудничество:*** цифровая трансформация не знает границ. Международное сотрудничество имеет важное значение, и стандарты должны способствовать глобальному сотрудничеству, гармонизации практик и правил, способствующих трансграничным инновациям и торговле.

Эти принципы являются компасом, указывающим направление в разработке и внедрении стандартов цифровой трансформации. Они не только способствуют эффективному управлению, но и служат дорожной картой для создания цифрового будущего, которое принесет пользу всем при решении сложных проблем нашего взаимосвязанного мира.

В реализации этих основополагающих принципов ключевую роль в формировании ландшафта цифровой трансформации играют различные устоявшиеся рамки и стандарты. Эти стандарты, благодаря своей полноте и эффективности, заняли свое место в качестве ориентиров в постоянно развивающуюся цифровую эпоху.

В данной комплексной публикации охватывается ряд важнейших рамочных документов и стандартов, представляя углубленное понимание их особенностей, спецификаций и правил. Первым стандартом, рассматриваемым в этой публикации, является Библиотека инфраструктуры информационных технологий (англ. Information Technology Infrastructure Library) (ITIL), известная своей эффективностью в управлении и оказании ИТ-услуг. ITIL играет ключевую роль в пропаганде передовых практик управления услугами, что делает ее бесценным ресурсом для организаций, стремящихся оптимизировать предоставление своих ИТ-услуг.

После ITIL представлена Архитектура взаимодействия электронного правительства (англ. e-Government Interoperability Framework). Эта архитектура призвана повысить интероперабельность и обмен данными в государственном секторе, обеспечивая не только доступность, но и высокую эффективность государственных услуг. Упор этой архитектуры на повышение доступности и эффективности играет важную роль в обеспечении эффективного государственного управления.

Далее в публикации рассматривается Методика описания архитектуры, разработанная Open Group (англ. The Open Group Architecture Framework, TOGAF) и Задачи управления для информационных и смежных технологий (англ. Control Objectives for Information and Related Technologies, COBIT). TOGAF обеспечивает комплексную методологию архитектуры предприятия, оптимизирующую проектирование, планирование, внедрение и управление ИТ-инфраструктурой организации. COBIT, с другой стороны, обеспечивает целостную основу для руководства и управления корпоративными ИТ, уделяя особое внимание управлению рисками, обеспечению ценности и оптимизации ресурсов.

Далее в работе представлен обзор Архитектуры взаимодействия электронного правительства (англ. e-Government Interoperability Framework) (e-GIF), основной целью которой является принятие спецификаций Интернета и Всемирной паутины для всех государственных систем. С помощью эталонной архитектуры облачных вычислений она предлагает организациям четко определенную эталонную архитектуру для реализации решений облачных вычислений. Эта архитектура служит ценным руководством, гарантирующим безопасное и эффективное внедрение облачных сервисов, помогая организациям использовать преимущества облачных технологий и одновременно снижать потенциальные риски.

Общий регламент по защите данных (англ. General Data Protection Regulation, GDPR) — еще один ключевой стандарт, представленный в настоящей публикации. GDPR стал глобальным эталоном в области регулирования защиты данных и конфиденциальности. Он устанавливает строгие стандарты защиты персональных данных физических лиц и налагает обязательства на организации, ответственные за обработку таких данных. Соблюдение GDPR имеет важное значение для организаций, работающих в Европейском Союзе и имеющих дело с персональными данными граждан ЕС.

В продолжение публикации представлен стандарт ISO/IEC 27001:2022. Этот международный стандарт ориентирован на системы управления информационной безопасностью и предлагает систематический подход к защите конфиденциальной информации. ISO/IEC 27001:2022 служит ценным ресурсом для организаций, стремящихся внедрить надежные методы информационной безопасности и эффективно защитить свои информационные активы.

Еще одним заслуживающим внимания рамочным документом является Система кибербезопасности (англ. Cybersecurity Framework), разработанная Национальным институтом стандартов и технологий (НИСТ; США). Она предоставляет организациям комплексные рекомендации по управлению и снижению рисков кибербезопасности. В мире, который становится все более цифровым и взаимосвязанным, эта система играет жизненно важную роль, помогая организациям укрепить свою позицию в области кибербезопасности и защититься от широкого спектра угроз.

В совокупности все эти стандарты представляют собой компоненты хорошо структурированной и безопасной цифровой среды, создавая основу для эффективного управления цифровой трансформацией, одновременно согласуясь с принципами надежности, инклюзивности, устойчивости, совместимости, безопасности, конфиденциальности данных и международного сотрудничества. Посредством их реализации мы можем решать сложные проблемы цифровой эпохи, гарантируя ответственное и справедливое использование выгод, обеспечиваемых технологиями.

I. Библиотека инфраструктуры информационных технологий (ITIL)

I.1. Введение

I.1.1 ITIL и его эволюция

ITIL представляет собой широко признанную основу для эффективного управления услугами ИКТ. Будучи направленной на повышение эффективности и качества услуг ИКТ, ее действие распространяется на различных поставщиков услуг, независимо от отрасли. Эта методология имеет прямое влияние на процессы, услуги и функции организации. Она помогает управлять услугами ИКТ как для внутренних, так и для внешних клиентов, предлагая необходимые навыки для достижения целей цифрового бизнеса.

Согласование ИКТ с бизнес-целями компании является сложной задачей, требующей профессиональных технологических возможностей. Основная цель технологического сектора – помочь организации в достижении ее основных целей.

Первоначально задуманная как аббревиатура «Библиотека инфраструктуры информационных технологий», ITIL превратилась в бренд, существующий уже три десятилетия. Хотя это больше не аббревиатура, она остается надежным руководством, охватывающим передовой опыт, который можно адаптировать. Эта методология признает различные профессиональные контексты, в которых работают организации, и поощряет гибкость при внедрении, соответствующем уникальным требованиям организации. Возникает вопрос: зачем управлять услугами ИКТ?

Управление информацией играет стратегическую роль в формировании бизнес-стратегии организации. Эффективное управление услугами ИКТ оптимизирует бизнес-процессы, повышая их эффективность и результативность при обработке важной информации. Более того, это способствует реализации разнообразных бизнес-моделей. Рассмотрим сценарий таких бизнес-структур, как банки, авиакомпании, платформы электронной коммерции и супермаркеты, а также государственных организаций, работающих без ИКТ. Становится очевидным, что таким организациям будет сложно функционировать без цифровых технологий. Предприятия в значительной степени зависят от ИКТ, и эта проблема характерна для разных организаций.

В настоящее время значительная часть бизнес-процессов опирается на ресурсы ИКТ, что подчеркивает их первостепенное значение в операционной деятельности. В то же время перебои в оказываемых услугах могут привести к серьезным последствиям. В условиях растущего спроса на услуги ИКТ среди организаций и предприятий подготовка технологических отделов часто отстает, что приводит к противоречию между спросом и предложением. Следовательно, тщательный анализ услуг ИКТ организации становится незаменимым в сочетании с постоянной бдительностью. В этом контексте цель данной публикации продемонстрировать, как методология ITIL может способствовать укреплению процессов и услуг ИКТ, тем самым расширяя возможности управления организацией.

Методология ITIL, зародившаяся в 1980-х годах под руководством Центрального агентства по вычислительной технике и телекоммуникациям (CCTA) британского правительства, представляла собой совокупность из более чем 30 книг, которые были подготовлены постепенно. В этих томах были систематически собраны лучшие практики ИТ, полученные со всего мира, включая вклад от поставщиков.

В апреле 2001 года CCTA был интегрирован в Управление государственной торговли (OGC), ныне известное как Кабинет министров. OGC принял проект ITIL, что согласовывалось с его миссией по сотрудничеству с государственным сектором Великобритании в повышении эффективности, оптимизации фискальной стоимости и повышении успеха в реализации программ и проектов.

В отличие от создания рыночного запатентованного продукта, стремление состояло в сборе лучших практик решения проблемы растущей зависимости правительства от ИТ, усугубляемой отсутствием стандартизированных процедур, которые приводили к росту затрат и распространению ошибок. Стало очевидно, что распространение этой практики будет выгодно как государственному, так и частному секторам.

Со временем авторитет ITIL укрепился. К 2005 году ITIL был согласован со стандартом управления услугами ISO/IEC 20000, первым международным стандартом управления ИТ-услугами, основанным на британском стандарте BS15000.

С 2013 года ITIL принадлежит Axelos, совместной организации Кабинета министров и Capita. Axelos предоставляет бизнес-лицензии на использование методологии ITIL, контролируя обновления и адаптацию процессов. Однако для внутреннего использования ITIL внутри организаций лицензии не требуются. В 2011 году был выпущен ITIL v3, в который были внесены изменения в версию OGC 2007 года.

Поворотный момент наступил в 2018 году, когда Axelos представила ITIL 4, явившейся существенной ревизией методологии с момента выпуска ITIL v3. Выпущенный в начале 2019 года ITIL 4 воплощает в себе гибкость, адаптируемость и кастомизацию, приспособленный для современных предприятий. Эта версия поддерживает взаимную связь, сотрудничество и интеграцию Agile и DevOps в стратегии управления ИТ-услугами.

I.1.2 Объяснение необходимости стандартизированных методов управления ИТ-услугами

Потребность в стандартизированных методах управления ИТ-услугами обусловлена сложной природой современного бизнеса и той важной ролью, которую информационные технологии (ИТ) играют в его деятельности. Стандартизированные методы управления ИТ-услугами предлагают структурированный и систематический подход к управлению ИТ-услугами. Они повышают эффективность, качество, управление рисками и сотрудничество, позволяя организациям соответствовать нормативным требованиям и адаптироваться к меняющимся потребностям бизнеса.

I.2. Обзор

I.2.1 Ключевые концепции, принципы и процессы

В основе структуры ITIL лежит несколько ключевых концепций, которые составляют ее философскую основу. Концепция ***«услуги»*** воплощает в себе суть предоставления ценности клиентам, подчеркивая ориентированный на клиента подход ITIL. ***«Управление услугами»*** включает в себя специализированные возможности организации, необходимые для эффективного создания, предоставления и управления этими услугами. Концепции ***«поставщик услуг»*** и ***«клиент»*** определяют отдельные роли и обязанности, обеспечивая четкое разграничение взаимодействия в услугах. Концепция ***«жизненного цикла услуги»*** располагает в определенном порядке последовательные этапы ITIL, помогая организациям в прохождении по всему пути управления услугами.

ITIL содержит комплекс руководящих принципов и направляет организации в достижении совершенства в управлении услугами. Принцип ***«фокусируйтесь на ценности»*** ставит во главу угла удовлетворенность клиентов и предоставление ценности. Принцип ***«Начинайте оттуда, где вы сейчас находитесь»*** поощряет постепенное улучшение, признавая имеющиеся возможности внутри организации. Принцип ***«Проектируйте для опыта»*** подчеркивает важность удовлетворенности пользователей и удобства использования. Принцип ***«Работайте целостно»*** требует сотрудничества между ИТ-подразделениями в целях бесперебойного предоставления услуг. Принцип ***«Итеративного развития»*** выступает за постоянное совершенствование, в то время как принципы ***«непосредственного наблюдения»*** и ***«поддержания прозрачности»*** подчеркивают важность обоснованного принятия решений и открытого общения. Аналогичным образом, принцип ***«Придерживайтесь простоты»*** подчеркивает важность простоты дизайна и эксплуатации.

Эти концепции и принципы прослеживаются во всех фундаментальных процессах ITIL. ***«Управление инцидентами»*** обеспечивает быстрое устранение сбоев, сводя к минимуму время простоя и негативное влияние на услуги. ***«Управление проблемами»*** углубляется в анализ первопричин для предотвращения повторяющихся инцидентов и повышения стабильности услуг. ***«Управление изменениями»*** контролирует внедрение изменений в услуги, снижение рисков и сбоев в услугах. ***«Управление уровнем услуг»*** направлено на определение и мониторинг уровня услуг для удовлетворения ожиданий клиентов. ***«Управление возможностями»*** оптимизирует использование ресурсов для эффективного предоставления услуг. ***«Управление доступностью»*** гарантирует доступность услуг за счет упреждающего устранения потенциальных сбоев. ***«Управление непрерывностью ИТ-услуг»*** обеспечивает устойчивость услуг в случае бедствий. ***«Финансовый менеджмент для ИТ-услуг»*** управляет ИТ-финансами в целях оптимизации затрат. ***«Управление конфигурацией»*** ведет точный учет ИТ-активов. ***«Управление релизами и развертыванием»*** обеспечивает плавное внедрение изменений. ***«Управление знаниями»*** собирает и распространяет организационные знания.

Таблица 1. Основные причины стандартизации практики управления ИТ-услугами

Аспект	Концепции и принципы
Последовательность и предсказуемость	Стандартизированные методы управления ИТ-услугами устанавливают единый подход к предоставлению услуг. Такая согласованность гарантирует, что услуги предоставляются предсказуемым образом, что приводит к повышению качества обслуживания клиентов и уменьшению сбоев.
Эффективность и производительность	Стандартизированные процессы устраняют избыточность, оптимизируют рабочие процессы и снижают вероятность ошибок. Такой оптимизированный подход повышает эффективность и производительность ИТ-операций.
Контроль качества	Стандартизированные методы основаны на проверенных методологиях и передовом опыте. Следование этим практикам обеспечивает более высокое качество обслуживания, сводя к минимуму риски ошибок и сбоев в услугах.
Управление рисками	Стандартизированные методы включают процедуры выявления, оценки и снижения рисков. Такой упреждающий подход помогает выявлять потенциальные проблемы до того, как они перерастут в серьезные проблемы.
Масштабируемость	Масштабы применения стандартизированных методов можно увеличивать или уменьшать в зависимости от меняющихся потребностей организации. По мере роста и развития бизнеса стандартизированные процессы обеспечивают постоянное качество услуг.
Межведомственное сотрудничество	Стандартизированные методы способствуют улучшению взаимодействия и сотрудничества между различными ИТ-командами и отделами. Такое согласование сводит к минимуму конфликты и обеспечивает взаимное понимание.
Соответствие нормативным требованиям	Многие отрасли подчиняются правилам и стандартам, связанным с безопасностью данных, конфиденциальностью и управлением ИТ. Стандартизированные методы помогают организациям соблюдать эти требования, избегая юридических и финансовых последствий.
Постоянное улучшение	Стандартизированные методы часто включают механизмы регулярного анализа и улучшения. Это позволяет обеспечить актуальность процессов, их соответствие отраслевым тенденциям и постоянную оптимизацию.
Сокращение времени обучения	Новые сотрудники могут быстро адаптироваться к стандартизированным процессам, если они следуют установленным правилам. Это сокращает время и ресурсы, необходимые для обучения и адаптации.
Повышение удовлетворенности клиентов	Постоянное предоставление услуг и более быстрое решение проблем приводят к более высокому уровню удовлетворенности клиентов. Соответствовать ожиданиям клиентов становится проще при наличии стандартизированных методов.
Бенчмаркинг и лучшие практики	Стандартизированные методы позволяют организациям сравнивать свою производительность с отраслевыми стандартами и передовой практикой. Это помогает определить области для улучшения и инноваций.
Управление изменениями	Стандартизированные методы обеспечивают структурированную основу для реализации изменений. Это сводит к минимуму влияние изменений на текущую деятельность и обеспечивает надлежащее тестирование и проверку.

I.2.2 Важность концепций и процессов: повышение качества предоставления и управления ИТ-услугами

Каждая концепция и процесс в ITIL вносят значительный вклад в улучшение предоставления ИТ-услуг и управления ими. Концепция ***«услуги»*** обращает внимание на ценность для клиента, подчеркивая, что услуги должны соответствовать бизнес-целям и потребностям клиентов. ***«Управление услугами»*** обеспечивает структурированный подход к созданию ценности, который объединяет процессы, людей, технологии и ресурсы. Различие между ***«Поставщиком услуг и клиентом»*** способствует четкому распределению ролей и ответственности, улучшая коммуникацию и сотрудничество. ***«Жизненный цикл услуги»*** предлагает целостную структуру для создания, предоставления, управления и улучшения услуг, обеспечивая стратегическую согласованность и постоянное совершенствование.

Процессы ITIL имеют огромное значение в управлении услугами. ***«Управление инцидентами»*** сводит к минимуму сбои, обеспечивая своевременное восстановление услуг. ***«Управление проблемами»*** устраняет коренные причины, предотвращая повторение инцидентов. ***«Управление изменениями»*** минимизирует риски при изменениях, сохраняя стабильность услуг. ***«Управление уровнем услуг»*** приводит ИТ-услуги в соответствие с бизнес-целями, повышая удовлетворенность клиентов. ***«Управление возможностями»*** оптимизирует использование ресурсов, предотвращая недостаточное или избыточное выделение ресурсов. ***«Управление доступностью»*** обеспечивает бесперебойную доступность услуг. ***«Управление непрерывностью ИТ-услуг»*** защищает услуги во время бедствий, поддерживая непрерывность бизнеса. ***«Управление финансами для ИТ-услуг»*** оптимизирует распределение ресурсов, обеспечивая экономическую эффективность. ***«Управление конфигурацией»*** обеспечивает точный учет ИТ-активов, облегчая управление изменениями. ***«Управление релизами и развертыванием»*** позволяет плавно вносить изменения, сокращая перебои в услугах. ***«Управление знаниями»*** способствует принятию решений и решению проблем, расширяя возможности организаций.

I.2.3 Архитектура ITIL и подход жизненного цикла

Центральным фактором эффективности ITIL является его подход жизненного цикла. Архитектура ITIL состоит из пяти этапов, каждый из которых представляет собой критическую фазу жизненного цикла услуги:

- ***Стратегия услуг:*** этот этап включает в себя понимание бизнес-целей, анализ потребностей рынка и создание стратегии услуг, которая согласует ИТ-услуги с бизнес-целями. Ключевые результаты включают портфель услуг, планы финансового управления и всестороннее понимание потребностей клиентов.
- ***Проектирование услуг:*** после этапа стратегии разрабатываются услуги для достижения установленных целей. Сюда входит разработка архитектурных планов, документации и процессов, которые гарантируют, что услуги принесут желаемую ценность. Результаты включают комплексные проекты услуг, соглашения об уровне услуг (SLA) и технологические аспекты.

- ***Преобразование услуг:*** этот этап обеспечивает плавное внедрение услуг при переходе от проектирования к рабочему состоянию. Мероприятия включают управление изменениями, тестирование, обучение и проверку. Ключевые результаты включают протестированные услуги, документированные изменения и учебные материалы.
- ***Эксплуатация услуг:*** после ввода в эксплуатацию услуги необходимо эффективно обслуживать и управлять ими. Этот этап включает в себя управление инцидентами, разрешение проблем и непрерывный мониторинг для поддержания производительности обслуживания. Результаты включают отчеты об инцидентах, решенные проблемы и показатели производительности.
- ***Постоянное улучшение услуг (CSI):*** на заключительном этапе особое внимание уделяется циклическому процессу оценки и улучшения. Анализ данных, оценка отзывов клиентов и действия по совершенствованию процессов приводят к обновлению процессов и планов. Результаты включают инициативы по улучшению, обновленную документацию и культуру постоянного улучшения.

I.2.4 Преимущества внедрения ITIL

Внедрение ITIL имеет множество преимуществ, которые отражаются на всей сфере ИТ-услуг организации:

- ***Повышение качества услуг:*** подход ITIL, ориентированный на клиента, гарантирует, что услуги соответствуют потребностям и ожиданиям клиентов, что приводит к более высокому качеству услуг и удовлетворенности.
- ***Соответствие бизнес-целям:*** подход жизненного цикла ITIL объединяет ИТ-стратегии с общими бизнес-целями, создавая прямую связь между ИТ-услугами и успехом организации.
- ***Снижение рисков:*** благодаря тщательному управлению изменениями и оценке рисков ITIL сводит к минимуму сбои, вызванные плохо управляемыми изменениями, что приводит к повышению стабильности и надежности предоставления услуг.
- ***Операционная эффективность:*** структурированные процессы и методы, поддерживаемые ITIL, оптимизируют операции, сокращают избыточность и оптимизируют распределение ресурсов, что приводит к повышению операционной эффективности.
- ***Сотрудничество и коммуникация:*** ITIL способствует сотрудничеству между различными ИТ-командами и отделами, способствуя беспрепятственному общению и обмену знаниями.
- ***Постоянное совершенствование:*** этот этап побуждает организации адаптировать и совершенствовать свои услуги на основе результатов аналитической обработки данных, что позволяет им оставаться актуальными в постоянно меняющейся среде.
- ***Четкая документация:*** ITIL требует четкого документирования процессов, процедур и сервисов, способствуя лучшему пониманию и облегчая более плавный переход.
- ***Адаптивность:*** итеративный характер ITIL позволяет организациям адаптироваться к меняющимся обстоятельствам, гарантируя, что услуги будут оставаться актуальными и эффективными с течением времени.

- ***Оптимизация затрат:*** приводя услуги в соответствие с потребностями бизнеса и улучшая использование ресурсов, ITIL помогает организациям оптимизировать затраты и добиваться более выгодной окупаемости инвестиций.
- ***Организационная согласованность:*** внедрение ITIL способствует развитию культуры сотрудничества и подотчетности, объединяя различные заинтересованные стороны для достижения общих целей предоставления услуг.

I.3. Роли и обязанности в ITIL

В ITIL (Библиотека инфраструктуры информационных технологий) роли и обязанности тщательно определены для обеспечения эффективного управления ИТ-услугами (ITSM). Эти роли составляют основу внедрения ITIL, предлагая структурированный подход к управлению услугами и процессами. Далее рассмотрим различные роли и обязанности, описанные в ITIL, с выделением таких ключевых позиций, как владелец услуги, владелец процесса и служба поддержки. В анализе подчеркивается важность ясности ролей и подотчетности в поддержании оптимизированного управления ИТ-услугами.

I.3.1 Изучение различных ролей и обязанностей в рамках ITIL:

- ***Владелец услуги:*** владелец услуги — это важная роль, отвечающая за общее управление и подотчетность конкретной ИТ-услуги на протяжении всего ее жизненного цикла. Он устраняет разрыв между ИТ и бизнесом, гарантируя, что услуга соответствует потребностям, целям и ожиданиям бизнеса. Владелец услуги наблюдает за стратегией услуги, ее проектированием, переходом, эксплуатацией и постоянным улучшением. Он сотрудничает с различными заинтересованными сторонами для определения требований к услуге, соглашений об уровне услуги и ключевых показателей эффективности.
- ***Владелец процесса:*** владельцы процессов несут ответственность за проектирование, эффективность и результативность конкретного процесса ITIL. Они гарантируют, что процессы хорошо задокументированы, соблюдаются и постоянно совершенствуются. Владельцы процессов работают над устранением узких мест, повышением эффективности и решением любых проблем в своих соответствующих процессах. Их роль включает в себя ведение документации процесса, настройку показателей производительности и улучшение процессов.
- ***Служба поддержки:*** служба поддержки, часто называемая «единой точкой контакта», — это группа, отвечающая за получение, регистрацию и управление инцидентами и запросами на обслуживание от пользователей. Они обеспечивают своевременные и точные ответы, устраняют проблемы и передают более сложные проблемы соответствующим командам. Служба поддержки выступает лицом ИТ-поддержки, обеспечивая эффективную связь и решение проблем для конечных пользователей.
- ***Менеджер изменений:*** менеджер изменений отвечает за контроль процесса управления изменениями. Они оценивают и утверждают изменения в ИТ-услугах, обеспечивая тщательную оценку изменений на предмет рисков, последствий и соответствия потребностям бизнеса. Менеджеры изменений помогают поддерживать стабильность услуг, предотвращая несанкционированные или плохо управляемые изменения, которые могут нарушить работу.

- ***Менеджер проблем:*** менеджер проблем фокусируется на предотвращении повторяющихся инцидентов, выявляя и устраняя коренные причины, анализируя данные об инцидентах, выполняя анализ тенденций и работая над внедрением постоянных исправлений, чтобы предотвратить возникновение подобных проблем в будущем. Роль менеджера проблем заключается в содействии улучшению качества услуг и уменьшению сбоев.
- ***Менеджер инцидентов:*** менеджер инцидентов отвечает за эффективную обработку и разрешение инцидентов, чтобы свести к минимуму перебои в услугах, а также определяет приоритетность инцидентов в зависимости от их воздействия и срочности, координирует усилия по разрешению инцидентов и передает обновления заинтересованным сторонам. Менеджеры инцидентов обеспечивают своевременное разрешение инцидентов и информирование конечных пользователей на протяжении всего процесса.

I.3.2 Важность ясности ролей и подотчетности в управлении ИТ-услугами

Основой успешного управления ИТ-услугами является четкость ролей и подотчетность отдельных лиц внутри организации. Такая ясность и подотчетность не только повышают эффективность и результативность ИТ-операций, но и способствуют развитию культуры сотрудничества и постоянного совершенствования. Давайте рассмотрим более подробно важность ясности в отношении ролей и подотчетности в управлении ИТ-услугами в различных аспектах.

- ***Эффективная коммуникация:*** четко определенные роли гарантируют, что обязанности хорошо понимаются во всей организации. Эта ясность способствует эффективному общению между командами, сводя к минимуму недоразумения и оптимизируя совместные усилия.
- ***Эффективные операции:*** ясность ролей предотвращает дублирование усилий и гарантирует, что задачи будут поручены соответствующим лицам или командам. Это приводит к более слаженной работе, сокращению задержек и оптимизации использования ресурсов.
- ***Подотчетность:*** четкие роли устанавливают подотчетность, делая очевидным, кто несет ответственность за конкретные задачи и результаты. Это способствует повышению ответственности и гарантирует выполнение задач на высоком уровне.
- ***Своевременное решение проблем:*** при наличии четко определенных ролей и обязанностей проблемы решаются оперативно нужными людьми. Это ускоряет разрешение инцидентов, сокращает время простоя и повышает удовлетворенность конечных пользователей.
- ***Следование процессам:*** такие роли, как владельцы процессов, обеспечивают поддержание в хорошем состоянии процессов и их последовательное следование им. Такое следование приводит к повышению эффективности процессов, соблюдению лучших практик и улучшению качества услуг.
- ***Комплексное управление услугами:*** такие роли, как владелец услуги, обеспечивают комплексное управление услугами, от их создания до прекращения. Такой подход приводит услуги в соответствие с потребностями бизнеса, что приводит к повышению удовлетворенности клиентов и повышению ценности.

Роли и обязанности в ITIL составляют основу эффективного управления ИТ-услугами. Эти роли, такие как владелец услуги, владелец процесса и служба поддержки, обеспечивают согласованное управление услугами и процессами, что приводит к оптимизации операций, эффективному разрешению инцидентов и культуре постоянного совершенствования. Четкость в распределении ролей способствует подотчетности, эффективным коммуникациям и эффективному использованию ресурсов, которые имеют первостепенное значение для предоставления высококачественных ИТ-услуг, соответствующих бизнес-целям. По мере того, как организации внедряют ITIL, внедрение четко определенных ролей становится важным для преодоления сложностей современных ИТ-ландшафтов и обеспечения устойчивого качества в предоставлении услуг и управлении ими.

I.4. Процесс внедрения

Внедрение ITIL (Библиотеки инфраструктуры информационных технологий) в организации является стратегическим начинанием, которое способствует эффективному и действенному управлению ИТ-услугами. Этот процесс включает в себя ряд шагов, от первоначальной оценки до полной интеграции, каждый из которых способствует согласованности ИТ-услуг с бизнес-целями. В этом обзоре описываются ключевые этапы принятия и внедрения ITIL, включая оценку, планирование, обучение и реализацию. Кроме того, здесь рассматриваются проблемы, с которыми организации могут столкнуться во время внедрения, и предлагаются стратегии для успешного внедрения.

I.4.1 Шаги по принятию и внедрению ITIL

При принятии и внедрении ITIL необходимо осознавать, что каждый шаг в процессе внедрения играет важную роль в достижении желаемых результатов. Эти шаги включают первоначальную оценку, детальное планирование, комплексное обучение, разработку процессов, пилотное внедрение, полномасштабное внедрение и стремление к постоянному совершенствованию. Такой системный подход не только обеспечивает более плавный переход, но и повышает вероятность успешной интеграции принципов ITIL в практику управления ИТ-услугами организации.

- ***Оценка:*** все начинается с оценки текущих практик управления ИТ-услугами в организации. Сюда входит оценка существующих процессов, выявление болевых точек и оценка готовности организации к изменениям. Сбор информации от заинтересованных сторон и понимание потребностей бизнеса имеют решающее значение для формирования стратегии внедрения ITIL.
- ***Планирование:*** после завершения этапа оценки организации приступают к комплексному планированию. Этот этап включает в себя определение объема внедрения, определение четких целей и определение стратегии интеграции практик ITIL. Создание проектной группы, распределение ролей и установление сроков являются важными компонентами этапа планирования.
- ***Обучение и осведомленность:*** организации должны инвестировать в обучение и повышение осведомленности среди своих сотрудников. ITIL основывается на общем понимании ролей, процессов и концепций, а надлежащее обучение обеспечит готовность всех участников к эффективному использованию практик

ITIL. Программы обучения могут варьироваться от базовых ознакомительных занятий до углубленных сертификационных курсов.

- ***Проектирование и настройка процессов:*** на этом этапе существующие процессы перепроектируются в соответствии с принципами ITIL. Организации настраивают процессы ITIL в соответствии со своими уникальными бизнес-потребностями и существующими рабочими процессами. Этот этап часто требует совместных усилий для обеспечения четкого определения, оптимизации процессов и повышения их эффективности.
- ***Пилотное внедрение:*** перед полномасштабным внедрением рекомендуется провести пилотный этап. Для этого практики ITIL внедряются в меньшем масштабе внутри конкретного отдела или службы. Пилотный этап позволяет протестировать и проверить процессы в контролируемой среде, что позволяет внести необходимые коррективы перед более широким внедрением.
- ***Внедрение и интеграция:*** используя уроки, извлеченные из пилотного этапа, организации осуществляют более широкое внедрение практик ITIL. Сюда входит внедрение новых процессов, обучение персонала и интеграция принципов ITIL в повседневную деятельность. На этом этапе решающее значение имеют непрерывный мониторинг и сбор обратной связи.
- ***Непрерывное совершенствование:*** заключительный этап включает в себя принятие принципа ITIL по постоянному улучшению услуг. Организации собирают данные, анализируют производительность и определяют области для улучшения. Этот циклический процесс обеспечивает развитие практик ITIL в соответствии с меняющимися потребностями бизнеса и достижениями в технологиях.

I.4.2 Проблемы и соображения по внедрению ITIL

Путь к успешной реализации сопряжен с рядом проблем и беспокойств, к решению которых организации должны быть готовы. Эти проблемы охватывают различные аспекты: от культурного сопротивления среди персонала до распределения ресурсов, управления изменениями и сложности адаптации практик ITIL. Преодоление этих препятствий необходимо для реализации всех преимуществ внедрения ITIL.

- ***Культурное сопротивление:*** изменение устоявшихся процессов может встретить сопротивление со стороны сотрудников. Преодоление сопротивления требует эффективной коммуникации, вовлечения ключевых заинтересованных сторон и демонстрации преимуществ внедрения ITIL.
- ***Распределение ресурсов:*** внедрение ITIL требует времени, усилий и ресурсов. Крайне важно обеспечить выделение адекватных ресурсов на обучение, перепроектирование процессов и постоянный мониторинг.
- ***Управление изменениями:*** внедрение ITIL является значительным организационным изменением. Внедрение надежных методов управления изменениями помогает решать проблемы, снижать риски и обеспечивать плавный переход.
- ***Управление сложностью:*** настройка процессов ITIL в соответствии с потребностями организации при сохранении простоты может оказаться сложной задачей. Баланс между сложностью и простотой использования жизненно важен для успешной реализации.

I.4.3 Стратегии успешного внедрения

Чтобы обеспечить отлаженное и успешное внедрение принципов ITIL в организации, можно использовать несколько стратегических подходов. Эти стратегии, начиная от поддержки со стороны руководства до эффективного обучения и постепенного внедрения, имеют важное значение для облегчения плавного перехода к практикам ITIL.

- ***Поддержка сверху вниз:*** приверженность руководства и создание благоприятных условий играют ключевую роль в обеспечении успешного внедрения ITIL. Поддержка со стороны руководства демонстрирует важность инициативы и побуждает других принять изменения.
- ***Эффективное обучение:*** комплексные программы обучения, адаптированные к различным должностям, улучшают понимание и принятие практик ITIL. Хорошо обученный персонал с большей вероятностью беспрепятственно внедрит новые процессы.
- ***Постепенное внедрение:*** внедрение ITIL поэтапно или начиная с пилотного проекта помогает снизить риски и позволяет осуществлять итеративные улучшения на основе реального опыта.
- ***Коммуникации и осведомленность:*** прозрачное информирование о преимуществах внедрения ITIL и о том, как оно соответствует бизнес-целям, способствует повышению заинтересованности сотрудников и других заинтересованных сторон.
- ***Непрерывный мониторинг и обратная связь:*** регулярно отслеживайте ход внедрения ITIL и собирайте отзывы пользователей. Это обеспечивает возможность внесения корректировок в реальном времени в ответ на поступающую информацию.

Принятие и внедрение ITIL в организации — это трансформационный путь, требующий тщательного планирования, обучения и исполнения. Описанные шаги, от оценки до постоянного улучшения, открывают путь к оптимизированному управлению ИТ-услугами в соответствии с бизнес-целями. Несмотря на возможные трудности, такие стратегии, как поддержка со стороны руководства, эффективное обучение, постепенное внедрение и непрерывный мониторинг, могут направить организации к успешному внедрению ITIL. Путем принятия принципов ITIL и их адаптации к уникальным потребностям организации, предприятия могут раскрыть потенциал для улучшения качества услуг, повышения эффективности и дальнейшего роста в динамичной сфере управления ИТ-услугами.

I.5. Практические примеры

В этой публикации рассмотрено широкое распространение и влияние Библиотеки инфраструктуры информационных технологий (ITIL) на управление ИТ-услугами в государственных организациях и в различных отраслях по всему миру.

Лидирующая роль Правительства Великобритании:

Идея ITIL пришла британскому правительству, и теперь она является официальной политикой, проводимой Управлением государственной торговли (OGC) правительства Великобритании. Правительство Великобритании начало использовать ITIL в 2005 году, и

это помогло им в значительной мере улучшить свои технологические услуги. Применение ITIL помогло сэкономить средства, обеспечить более высокий уровень удовлетворенности клиентов, лучше соблюдать правила и больше сосредоточиться на том, что нужно клиентам.

Государственная поддержка и правила:

Именно правительства стали основной причиной популярности ITIL. В США некоторые правительственные группы заставляют компании получать сертификаты ITIL. В Австралии правительство советует своим группам использовать ITIL для улучшения технологий. Внедрение ITIL началось с государственного сектора, но теперь ее используют и многие частные компании.

Преимущества, наблюдаемые во всем мире:

Во многих странах, таких как Австралия, Новая Зеландия, Сингапур и ОАЭ, также применяется ITIL. Было обнаружено, что это помогло тратить меньше средств на технологии, обеспечить более высокий уровень удовлетворенности клиентов, работать быстрее и лучше, снизить риски и обеспечивать соблюдение правил. В результате этих преимуществ библиотека ITIL стала широко известна как способ улучшения технологических услуг.

Мировое влияние:

Крупные компании, такие как Procter & Gamble и General Motors, используют ITIL для получения технологических услуг из других стран, особенно из таких стран, как Индия. Они хотят, чтобы компании, с которыми они работают, также имели сертификацию ITIL. Подводя итог, можно сказать, что путь ITIL от правительственной инициативы до глобального явления иллюстрирует ее непреходящую ценность в оптимизации управления ИТ-услугами. Принципы ITIL продолжают помогать организациям в стремлении к более эффективному, ориентированному на клиента и совместимому предоставлению технологических услуг. Это делает ITIL важным и неотъемлемым инструментом в современной цифровой среде.

I.6. Выводы

В заключение следует отметить, что Библиотека инфраструктуры информационных технологий (ITIL) является ключевым стандартом для управления ИТ-услугами, предлагая структурированный и комплексный подход к согласованию технологических услуг с целями организации. Эта концепция, которая развивалась на протяжении трех десятилетий, стала глобальным стандартом, принятым правительствами, государственными и частными организациями, а также предприятиями различных масштабов. Успех ITIL можно объяснить клиентоориентированным подходом, акцентом на совершенствование процессов и адаптируемостью к различным отраслевым контекстам.

Основные концепции и принципы ITIL, такие как ориентация на ценность, постоянное совершенствование и четкое определение ролей, обеспечивают прочную основу для улучшения предоставления ИТ-услуг и управления ими. Фундаментальные процессы

стандарта, включая управление инцидентами, управление проблемами и управление изменениями, предлагают практические решения для распространенных проблем ИТ-услуг.

Подход жизненного цикла ITIL, включающий в себя стратегию услуг, проектирование услуг, преобразование услуг, их эксплуатацию и постоянное улучшение, помогает организациям пройти целостный путь по управлению услугами. Каждый этап играет решающую роль в обеспечении не только эффективности ИТ-услуг, но и стратегического соответствия бизнес-целям.

Внедрение ITIL — это стратегическое мероприятие, требующее тщательного планирования, обучения и постепенной интеграции. Хотя могут возникнуть такие проблемы, как культурное сопротивление и распределение ресурсов, такие стратегии, как поддержка сверху вниз, эффективное обучение и постоянный мониторинг, могут способствовать успешному внедрению.

Практические примеры демонстрируют широкое влияние ITIL на управление ИТ-услугами, при этом именно правительства лидируют в ее внедрении. От новаторского использования ITIL правительством Великобритании до транснациональных корпораций, добивающихся сертификации ITIL для своих поставщиков услуг, этот стандарт доказал свою эффективность в улучшении качества услуг, повышении их эффективности и степени соответствия потребностям клиентов.

Подводя итоги, ITIL стал фундаментальным элементом управления ИТ-услугами, предлагая организациям план действий по предоставлению высококачественных услуг, снижению рисков и развитию культуры постоянного совершенствования. В условиях постоянного развития технологий ITIL остается ценным инструментом для организаций, которые стремятся ориентироваться в сложных условиях современных ИТ-ландшафтов, обеспечивая, тем самым, превосходство в предоставлении услуг и управлении ими.

I.7. Краткое резюме

Эволюция ITIL: ITIL, первоначально задуманный как «Библиотека инфраструктуры информационных технологий», за три десятилетия превратился во всемирно признанный стандарт управления ИТ-услугами. Из аббревиатуры он превратился в бренд, предлагающий адаптируемые лучшие практики.

Важность управления ИТ-услугами: эффективное управление ИТ-услугами имеет решающее значение для организаций, поскольку информационные технологии играют стратегическую роль в формировании бизнес-стратегий, оптимизации процессов и обеспечении эффективности и результативности.

Ключевые концепции и принципы: ITIL руководствуется такими ключевыми концепциями, как «услуга», «управление услугами», «поставщик услуг» и «клиент», а также такими принципами, как «ориентация на ценность» и «постоянное улучшение».

Фундаментальные процессы: ITIL описывает фундаментальные процессы, включая управление инцидентами, управление проблемами, управление изменениями,

управление уровнем услуг и многие другие, каждый из которых способствует эффективному предоставлению услуг и управлению ими.

Жизненный цикл ITIL: структура ITIL соответствует концепции жизненного цикла, включающему стратегию услуг, проектирование услуг, преобразование услуг, их эксплуатацию и постоянное улучшение, обеспечивая стратегическое согласование и постоянное улучшение ИТ-услуг.

Преимущества внедрения ITIL: организации, внедряющие ITIL, получают выгоды от повышения качества услуг, соответствия бизнес-целям, снижения рисков, повышения операционной эффективности, улучшения сотрудничества и культуры постоянного совершенствования.

Роли и обязанности: ITIL определяет ключевые роли, такие как владелец услуги, владелец процесса, служба поддержки, менеджер изменений, менеджер проблем и менеджер инцидентов, каждая из которых способствует эффективному управлению ИТ-услугами за счет ясности ролей и подотчетности.

Процесс внедрения: внедрение ITIL включает в себя такие этапы, как оценка, планирование, обучение, проектирование процессов, пилотное внедрение, реализацию и постоянное совершенствование, с учетом решений проблем и обеспечения успешного внедрения.

Глобальное воздействие: правительства во всем мире сыграли значительную роль в продвижении внедрения ITIL, при этом организации в разных странах получили такие преимущества, как экономия затрат, повышение степени удовлетворенности клиентов и улучшение управления рисками.

Актуальность: ITIL остается актуальным и адаптируемым к развивающимся технологическим ландшафтам, что делает его ценным ресурсом для организаций, стремящихся разобраться в сложностях управления ИТ-услугами.

Эволюция ITIL, основные понятия, принципы, процессы и концепция жизненного цикла предлагают организациям структурированный путь к достижению совершенства в предоставлении и управлении ИТ-услугами, а практические примеры из реальной жизни демонстрируют его глобальное влияние и сохраняющуюся актуальность.

I.8. Список литературы

- ITIL Foundation: ITIL 4 edition (2019). London: TSO.
- Lopes, S.F. (2021) 'The importance of the ITIL framework in managing information and Communication Technology Services', International Journal of Advanced Engineering Research and Science, 8(5), pp. 292–296. doi:10.22161/ijaers.85.35.
- Marrone, M., Gacenga, F., Cater-Steel, A., & Kolbe, L. (2014). IT Service Management: A Cross-national Study of ITIL Adoption. Communications of the Association for Information Systems, 34, pp-pp. https://doi.org/10.17705/1CAIS.03449
- What is itil? your guide to the IT infrastructure library (2022) CIO. https://www.cio.com/article/272361/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html
- White, S.K. and Greiner, L. (no date) 'What is ITIL? Your guide to the IT Infrastructure Library'.
- 20 benefits of IT Service Management (ITSM) (2023) Ivanti, https://www.ivanti.com/blog/benefits-of-it-service-management

II. Архитектура взаимодействия электронного правительства (e-GIF)

II.1. Введение

По мере развития электронного правительства становится все более важным обеспечение совместимости между различными услугами и информационными системами. Для качественных государственных услуг, адаптированных к потребностям граждан и бизнеса, необходим беспрепятственный поток информации через правительство. Согласно Европейской структуре совместимости (EIF), термин «совместимость» (или «интероперабельность») означает способность организаций взаимодействовать для достижения взаимовыгодных целей, включая обмен информацией и знаниями между ними через бизнес-процессы, которые они поддерживают, посредством обмена данными в системах информационных и коммуникационных технологий (ИКТ).

Правительства многих стран постоянно работают над повышением совместимости электронного правительства. Показательным примером является e-GIF в Великобритании. Архитектура взаимодействия электронного правительства (e-GIF) определяет техническую политику и спецификации правительства для достижения функциональной совместимости и согласованности систем ИКТ в государственном секторе. e-GIF определяет основные предпосылки для объединенного правительства, работающего через Интернет. e-GIF является фундаментальным техническим документом электронного правительства для электронного объединения государственного сектора и предоставления современных, улучшенных государственных услуг. Он является прагматичным интернет-подходом для снижения затрат и рисков. Это позволяет организациям государственного сектора сконцентрироваться на обслуживании клиентов посредством информации и услуг с добавленной стоимостью.

Соблюдение политик и спецификаций e-GIF является обязательным. Основной целью e-GIF является принятие спецификаций Интернета и Всемирной паутины (WWW) для всех государственных систем. e-GIF также определяет политику создания и внедрения метаданных в государственном секторе. Однако само по себе определение политики и спецификаций недостаточно. Успешная реализация будет означать предоставление поддержки, рекомендаций по передовому опыту, наборов инструментов и централизованно согласованных схем. На сайте GovTalk (Схемы и стандарты) представлены рекомендации по передовому опыту, часто задаваемые вопросы (FAQ), советы по обучению и наборам инструментов, а также описаны процессы управления[1].

Впервые документ e-GIF вступил в силу после объявления в 2000 году Версии 1 в Палате общин (Великобритания), последняя версия, версия 6.1, была выпущена в марте 2005 года. В настоящее время многие страны применяют e-GIF в соответствии со своими потребностями[2] или разрабатывают и применяют другие методологии обеспечения

---

[1] GovTalk Кабинета министров Великобритании. Схемы и стандарты; https://webarchive.nationalarchives.gov.uk/ukgwa/20111205165431/http://interim.cabinetoffice.gov.uk/govtalk/schemasstandards.aspx

[2] Национальный архив. (2005). Кабинет министров. Архивные документы e-GIF — Название: Архитектура взаимодействия электронного правительства, версия 6.1. https://webarchive.nationalarchives.gov.uk/ukgwa/20111205214947/http://interim.cabinetoffice.gov.uk/govtalk/archive/policy_documents_1_of_1/e-gif/e-gif_published_documents/e-government_interoperability_framework_version_61.aspx

совместимости. В настоящей публикации сначала описывается e-GIF (версия 6.1), а затем другие виды методологий обеспечения совместимости.

II.2. Обзор Архитектуры взаимодействия электронного правительства (e-GIF)

II.2.1 Определение e-GIF

Архитектура взаимодействия электронного правительства (e-GIF) была разработана кабинетом министров Великобритании, который признал необходимость беспрепятственного потока информации в правительстве для улучшения удовлетворения потребностей граждан и бизнеса. e-GIF устанавливает государственную техническую политику и спецификации для достижения функциональной совместимости и согласованности систем ИКТ в государственном секторе.

e-GIF представляет собой набор политик и стандартов, обеспечивающих беспрепятственный обмен информацией в государственном секторе и предоставляющий гражданам и предприятиям улучшенный доступ к государственным услугам. Документ e-GIF состоит из шести разделов:

- (Раздел 1) Политика и сфера применения;
- (Раздел 2) Техническая политика;
- (Раздел 3) Поддержка по внедрению;
- (Раздел 4) Процессы управления;
- (Раздел 5) Управление изменениями;
- (Раздел 6) Обеспечение соответствия e-GIF.

Политика и сфера применения e-GIF заключаются в следующем.

- Современному объединенному правительству требуются объединенные (совместимые) системы ИКТ.
- Содержит четко определенные политики и спецификации для взаимодействия и управления информацией.
- Легко доступные и передаваемые между государственным и частным секторами информационные ресурсы с учетом обязательств по конфиденциальности и безопасности.

e-GIF определяет минимальный набор технических политик и спецификаций, регулирующих потоки информации в правительстве и государственном секторе. Они охватывают взаимосвязь, интеграцию данных, метаданные управления контентом и доступ к электронным услугам. Правительство стремится обеспечить постоянное соответствие этой политики и спецификаций изменяющимся требованиям государственного сектора, а также развитию рынка и технологий.

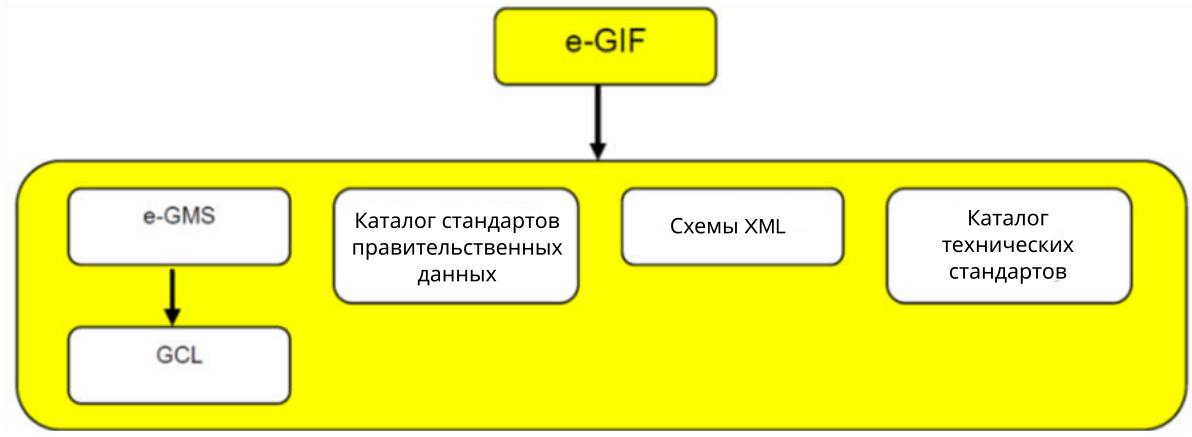
II.2.2. Структура e-GIF

II.2.2.1 Архитектура e-GIF

Архитектура e-GIF содержит:

- Рамочную основу, которая охватывает политические заявления высокого уровня, техническую политику и режимы управления, реализации и обеспечения соответствия;
- Реестр e-GIF, который охватывает стандарт метаданных электронного правительства (e-GMS) и список государственных категорий (GCL), каталог стандартов государственных данных (GDSC), схемы XML и каталог технических стандартов (TSC).

Рис. 1: Архитектура e-GIF



Ключевые политические решения, которые сформировали e-GIF:

- Присоединение к Интернету.
- Внедрение XML (расширяемый язык разметки).
- Принятие браузера в качестве основного интерфейса.
- Добавление метаданных в государственные информационные ресурсы.
- Разработка и внедрение e-GMS (Стандарта метаданных электронного правительства Великобритании), основанного на международной модели Dublin Core (ISO 15836).
- Разработка и поддержка GCL (Списка категорий правительства).
- Соблюдение e-GIF является обязательным во всем государственном секторе.
- Интерфейсы между государственными информационными системами и посредниками, предоставляющими услуги электронного правительства, должны соответствовать стандартам e-GIF.

Выбор спецификаций e-GIF был обусловлен интероперабельностью, поддержкой рынка, масштабируемостью, открытостью и международными стандартами. e-GIF охватывает обмен информацией между государственными системами и взаимодействие между правительством Великобритании и гражданами, посредниками, предприятиями (по всему миру), организациями в правительстве Великобритании, правительствами других стран, например, Великобритании/ЕС, Великобритании/США и т.д.

Обязательное соблюдение e-GIF применяется только к государственному сектору Великобритании. Однако стандарты e-GIF также влияют на информационные системы государственного сектора Великобритании, а также информационные системы частного сектора и других стран. Таким образом, несмотря на то, что обязательства по соблюдению требований e-GIF не могут быть наложены на граждан, предприятия и иностранные правительства, правительство Великобритании ясно дает понять всем, что он является предпочитаемым методом взаимодействия.

II.2.2.2 e-GMS

Вставка 1: Основные документы, относящиеся к e-GMS.

1. e-GMS 3.1
2. e-GMS версия 3.1 для веб-сайтов
3. e-GMS Схема кодирования – Тип 1.0
4. e-GMS Схема кодирования – Целевая аудитория (проект)

Поскольку объединенному правительству необходимы объединенные информационные системы, Стандарт метаданных электронного правительства (e-GMS), как часть e-GIF, необходим для обеспечения максимальной согласованности метаданных в организациях государственного сектора. Стандарт (e-GMS) устанавливает элементы, уточнения и схемы кодирования, которые будут использоваться государственными служащими при создании метаданных для своих информационных ресурсов или при разработке поисковых систем для информационных систем.

II.2.2.3 Каталог государственных стандартов данных (GDS)

Вставка 2: Меню данных GDS

- Адрес
- Контактная информация
- Финансовые идентификаторы
- Информация об организации
- Информация о человеке.
- Прочее
- Связи

Архитектура взаимодействия электронного правительства (e-GIF) предписывает принятие XML и разработку схем XML в качестве основного компонента стратегии взаимодействия и интеграции правительства. Ключевым элементом разработки схем XML является согласованный набор стандартов данных. Согласованный набор государственных стандартов данных (GDS), которые будут использоваться в схемах и других процессах обмена, содержится в Каталоге стандартов данных. Эти стандарты также рекомендуются для хранения данных на бизнес-уровне.

II.2.2.4 XML-схемы

Многие государственные процессы включают обмен данными. Следовательно, для понимания данных, которыми обмениваются между информационными системами, применяются схемы. В основе этих обменов данными лежат схемы XML, которые представляют собой общие определения данных, которые GovTalk определил для использования во всем государственном секторе[3].

[3] Схемы делятся на четыре области: (1) Библиотека схем; (2) Поиск схем; (3) Руководство для разработчиков; и (4) Форма запроса схемы. Доступ к дополнительным основным схемам доступен в Каталоге стандартов данных правительства Великобритании, дополнительные документы, касающиеся схем, можно найти в разделе «Руководство для разработчиков». Дополнительную информацию можно найти в разделе «Процедуры контроля изменений для ресурсов электронного правительства».

II.2.2.5 Каталог технических стандартов

Каталог технических стандартов определяет минимальный набор спецификаций, соответствующих технической политике, определенной в e-GIF[4].

II.2.2.6 Техническая политика

В этом разделе описываются подробные технические политики в отношении межсетевых соединений, интеграции данных, метаданных управления контентом и доступа к электронным услугам. Также включена техническая политика для сфер деятельности[5]. Последняя спецификация TSC приведена в Приложении 1 к настоящему отчету и охватывает такие вопросы как межсетевые соединения, интеграция данных, метаданные управления контентом и доступа к электронным услугам, спецификации для сфер деятельности и приложений. Каждая область содержит таблицы со спецификациями, номерами версий и примечаниями. Правительство Великобритании стремится обеспечить соответствие этой технической политики и спецификаций меняющимся требованиям государственного сектора, а также изменениям на рынке и в технологиях

В Разделе 2 в e-GIF версии 6.1 объясняется общая техническая политика для каждой части – Взаимосвязи; Посредники; Переход на IPv6; Беспроводные локальные сети; Интеграция данных; Формы; Метаданные управления контентом; Идентификаторы; доступ и каналы электронных услуг; Каналы; Стандарты по направлениям деятельности. Подробные спецификации представлены в виде отдельной таблицы. Ниже приведен пример технической политики в области межсетевых соединений.

Вставка 3: Межсетевые соединения (Пример технической политики)

Техническая политика межсетевых соединений охватывает следующее:
2.3 В правительстве нормой будет использование внутренней безопасности, обеспечиваемой правительственным безопасным интранетом (GSI), для обеспечения конфиденциальности электронной почты. Если требования безопасности не требуют иного, за пределами GSI и других защищенных государственных сетей должно использоваться одно из следующего: S/MIME или стандарты безопасной почты и безопасного доступа к почте, защищенные с использованием как минимум 128-битных соединений TLS/SSL.

[4] Национальный архив. (2010). Кабинет министров. Каталоги технических стандартов (TSC)-TSC Содержание. https://webarchive.nationalarchives.gov.uk/ukgwa/20111205171942/http://interim.cabinetoffice.gov.uk/govtalk/schemasstandards/e-gif/technical_standards_catalogue.aspx

[5] Последние технические спецификации этих политик см. в Каталоге технических стандартов (TSC, версия 6.2), который также содержит глоссарий сокращений и аббревиатур, используемых в e-GIF. Национальный архив. (2009). Кабинет министров. Опубликованные документы E-GIF — Каталог технических стандартов, версия 6.2. https://webarchive.nationalarchives.gov.uk/ukgwa/20111205175001/http://interim.cabinetoffice.gov.uk/govtalk/schemasstandards/e-gif/tsc_rtf_and_pdf_versions.aspx

Таблица 2: Пример таблицы TSC (спецификации межсетевого взаимодействия)

Компонент	Спецификация	Статус
Протоколы передачи гипертекста	RFC 2616, Механизм обновления HTTP/1.1 для инициирования безопасности транспортного уровня (TLS) через существующее TCP-соединение.	A
Передача электронной почты	Продукты электронной почты, поддерживающие интерфейсы, соответствующие SMTP/MIME для передачи сообщений. Сюда входят RFC 2821, RFC 2822, RFC 2045, RFC 2046, RFC 2646, RFC 2047, RFC 2231, RFC 2048, RFC 3023, RFC 2049. *Прим. Вложения электронной почты могут соответствовать типам файлов для браузеров и программ просмотра в соответствии с определенным для конкретного канала доставки см. в Разделе 7 – Доступ к электронным услугам и каналы.*	A
Транспортная безопасность	SSL v3/TLS (RFC 2246)	A

II.2.2.7 Поддержка внедрения и т.д.

Разделы 3–6 e-gif необходимы для внедрения, управления, изменения и соблюдения e-gif. В таблице 2 приведены содержание и структура.

Таблица 3. Краткое описание содержания разделов 3-6 e-GIF.

Раздел	Содержание	Вопросы
3. Поддержка внедрения	Процессы, с помощью которых e-GIF и инструменты, необходимые для его реализации, будут разрабатываться, применяться и поддерживаться.	• Приоритеты. • Создание XML-схемы. • Стандарт метаданных электронного правительства. • www.govtalk.gov.uk . • Членство в рабочих группах.
4. Процессы управления	Изложены роли и обязанности центрального правительства и других организаций государственного сектора и отрасли. Указаны основные функции, без претензии на то, что информация является исчерпывающей.	• Отдел электронного правительства. • Организации государственного сектора. • Промышленность. • Граждане. • ИТ-форум. • Рабочая группа по интероперабельности. • Группа по правительственным схемам. • Рабочая группа по метаданным. • Рабочая группа по смарт-картам. • Другие рабочие группы.

Раздел	Содержание	Вопросы
5. Управление изменениями	Спецификации e-GIF неизбежно будут меняться, и при необходимости их можно будет быстро изменить. Процесс управления изменениями должен обеспечить сохранение актуальности e-GIF и его соответствия требованиям всех заинтересованных сторон, а также потенциалу новых технологий и развития рынка. *Описывается инклюзивный процесс консультаций через Интернет, который будет способствовать участию и инновациям. Также описывается как будет осуществляться управление изменениями в спецификациях ресурсов электронного правительства.*	• Владелец ресурса электронного правительства. • Срок существования ресурса электронного правительства. • Консультации и инновации. • Запрос комментариев. • Запрос предложений. • Обновления e-GIF.
6. Соблюдение e-GIF	Политики e-GIF требуют соблюдения TSC и e-GMS, и в этом разделе представлены общие рекомендации о том, что означает соответствие в этом контексте и как оно будет обеспечиваться. Также включены функции в частных/коммерческих организациях, которые разрабатывают и/или предоставляют лицензированные государственные услуги.	• Что означает соответствие e-GIF? • Использование XML-схем и стандартов данных. • График. • Заинтересованные стороны. • Обязанности по соблюдению требований. • Сообщества государственного сектора. • Поддержание соответствия новым версиям e-GIF. • Несоблюдение. • Дополнительные рекомендации.

II.2.3 Статус различных рамочных стандартов по интероперабельности

В этой части представлена политика обеспечения интероперабельности государственных информационных систем в различных странах. Политика интероперабельности в каждой стране принимает различные формы в зависимости от прогресса каждой страны в области электронного правительства или от уровня применения политики (более подробная информация представлена в части, где рассмотрены примеры конкретных стран (кейсы).

Во-первых, политика обеспечения интероперабельности с точки зрения архитектуры впервые была начата в США, и ее также применяли другие страны, такие как Корея. США и Корея установили политику обеспечения интероперабельности на основе архитектуры предприятия (EA). В этих странах назначен директор по информационным технологиям (CIO), в обязанности которого входит создание EA и обеспечение интероперабельности.

В других случаях (например, X-load в Эстонии и Архитектура электронного правительства в Корее) страны создали не просто политику или рекомендации, а общегосударственную информационную и коммуникационную инфраструктуру для обеспечения интероперабельности. Эстония (X-tee) и Корея (система обмена публичной информацией) создают общую инфраструктуру для соединения данных и услуг и посредством этого обеспечивают интероперабельность. В частности, Корея улучшает интероперабельность на уровне программного обеспечения и приложений путем разработки общей структуры – Рамочного стандарта электронного правительства, связанного с разработкой систем.

Таблица 4: Текущая политика и законы в отношении данных в ведущих странах[6]

Категория	США	Китай	ЕС	Великобритания	Япония	Австралия
Основные политики	Федеральная стратегия данных (FDS)	14-й пятилетний план развития индустрии больших данных	Европейская стратегия данных	Национальная стратегия в области данных (NDS)	Комплексная стратегия в области данных	Австралийская стратегия в области данных
Агентство, ответственное за развитие индустрии данных	Совет CDO, Совет директоров по данным	Министерство промышленности и информационных технологий	ЕК, Европейская комиссия	Департамент цифровых технологий, культуры, медиа и спорта	Цифровое агентство	Агентство цифровой трансформации
Детальная политика	План действий Федеральной стратегии в области данных; Инициатива по оптимизации дата-центров	Пилотный проект по развитию индустрии больших данных	Европейское облако открытой науки	Программа «Data First»	Карта «My number»	Инициатива по инфраструктуре исследовательских данных
Детальная политика	План действий Федеральной стратегии в области данных; Инициатива по оптимизации дата-центров	Пилотный проект по развитию индустрии больших данных	Европейское облако открытой науки	Программа «Data First»	Поправка к Закону о защите персональной информации; Основной закон о формировании цифрового общества; Основной закон о совершенствовании	Инициатива по инфраструктуре исследовательских данных

[6] Корейское агентство данных. Резюме информационного документа по индустрии данных за 2022 год. https://www.kdata.or.kr/filedownload.do;jsessionId=86aab35b8638019723892fcbbb87c1bf9?srvfile=202302211533356368O.pdf--&22212115333563680.pdf&usrfile=2022115333563680.pdf&usrfile=2022115323563680.pdf&usrfile=2022115333563680.pdf&usrfile=2022121153335630. Summary.pdf & Folder = WhitePaper

Категория	США	Китай	ЕС	Великобритания	Япония	Австралия
					использования данных государственного и частного секторов	
Функции	Помощь федеральным агентствам в расширении своих возможностей обработки данных	Государственное нисходящее развитие отрасли	Создание	Активная поддержка трансграничного потока данных	Содействие государственно-частному сотрудничеству на основе административных данных	Разработка политики, объединяющей существующие политики и правовые системы.

** В США нет общегосударственного закона о конфиденциальности.*

В последнее время, когда важность данных становится все более актуальной, правительства стран разрабатывают национальные стратегии в области данных и политику для обеспечения их совместимости. Учитывая обширный и разнообразный характер политик в разных странах, здесь мы приведем лишь краткое резюме таких политик.

II.2.3. 1 Европейский свод требований по совместимости

В ноябре 2022 года Европейской комиссией (ЕК) был предложен Закон о совместимой Европе (англ. Interoperable Europe Act) в целях повышения совместимости в государственном секторе. Функциональная совместимость позволяет администрациям сотрудничать и обеспечивать функционирование государственных услуг независимо от территориальных, отраслевых и организационных границ, при этом администрации остаются суверенными субъектами на всех уровнях государственного управления[7].

Планы Европейского Союза (ЕС) в области цифровизации до 2030 года и сохраняющиеся пробелы в фактическом обеспечении совместимости продемонстрировали необходимость создания усиленной и более стратегической политики совместимости с усилением сотрудничества между государствами-членами и институтами ЕС по вопросам совместимости в государственном секторе.

«Европейский свод требований по совместимости» (англ. - European Interoperability Framework, EIF)» является частью документа «Communication – COM (2017) 134», принятого Европейской комиссией 23 марта 2017 года[8]. Свод содержит конкретные рекомендации

[7] Европейская комиссия. «Объединяйтесь – совместимая Европа – политика». Политика совместимой Европы. https://joinup.ec.europa.eu/interoperable-europe/policy

[8] Европейская комиссия. Новый европейский свод требований по совместимости; https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf ; https://ec.europa.eu/isa2/sites/default/files/eif_leaflet_final.pdf
Европейская комиссия. ISA2 – Новый европейский свод требований по совместимости. https://ec.europa.eu/isa2/eif_en/

по созданию совместимых цифровых государственных услуг. Он предлагает государственным органам конкретные рекомендации о том, как улучшить управление их деятельностью по обеспечению совместимости, установить межорганизационные отношения, оптимизировать процессы поддержки сквозных цифровых услуг и обеспечить, чтобы как существующее, так и новое законодательство не ставили под угрозу усилия по обеспечению совместимости. Успешная реализация EIF позволит повысить качество европейских государственных услуг и создать среду, в которой государственные органы смогут сотрудничать в цифровом формате.

EIF сопровождается Планом действий по обеспечению совместимости, в котором изложены приоритеты, направленные на поддержание реализации EIF с 2016 по 2020 год. План действий по обеспечению совместимости состоит из пяти основных направлений, в которых рассматриваются вопросы, связанные с определением механизмов управления совместимостью, сотрудничеством между организациями, вовлечением заинтересованных сторон и повышением осведомленности о преимуществах совместимости. Он также охватывает разработку, улучшение и продвижение ключевых средств обеспечения совместимости с учетом потребностей и приоритетов конечных пользователей.

II.2.3.2 X-Road (X-tee)

X-Road, программное обеспечение и экосистемное решение с открытым исходным кодом, которое обеспечивает унифицированный и безопасный обмен данными между организациями частного и государственного сектора, является основой электронной Эстонии[9]. Будучи незаметным, но крайне важным, оно позволяет различным государственным и частным информационным системам электронных услуг объединяться и гармонично функционировать. Эстонская среда X-Road «X-tee», откуда и произошло название X-Road, включает в себя полный спектр услуг для широкой публики, и поскольку каждая услуга имеет собственную информационную систему, все они полагаются на X-Road. Чтобы обеспечить безопасную передачу, все исходящие данные снабжаются цифровой подписью и шифруются, а все входящие данные аутентифицируются и регистрируются.

X-Road объединяет различные информационные системы, которые могут включать в себя множество сервисов. Он превратился в инструмент, который также может обращаться в несколько информационных систем, передавать большие наборы данных и выполнять поиск в нескольких информационных системах одновременно. X-Road был разработан с учетом роста, поэтому его можно масштабировать по мере появления в сети новых электронных услуг и платформ. X-Road обеспечивает надежное и безопасное решение для обмена данными и создания совместной экосистемы. Оно оптимизирует процессы

---

[10]После обретения независимости Эстония построила свою национальную административную систему на цифровой основе и создала основу для обмена данными в Интернете. Поскольку физически построить административную систему (например, построить новое правительственное учреждение и т. д.) было сложно, более реалистичным было сделать выбор в пользу цифровых технологий. Признавая, что обмен данными является фактором, обеспечивающим безопасное и эффективное национальное управление, мы внедрили основанные на этом инновационные услуги и создали эффективный цикл развития цифровых услуг.
электронная Эстония. Услуги по совместимости - X-ROAD. https://e-estonia.com/solutions/interoperability-services/x-road/

обмена данными, повышает безопасность и облегчает взаимодействие, позволяя организациям извлекать большую выгоду из своих информационных активов.

II.2.3.3 Архитектура предприятия (EA)

Согласно «Руководству по совместимости электронного правительства» ПРООН[11], в достижении совместимости посредством GIF и их стандартов архитектура играет важную роль в обеспечении успеха в области интероперабельности электронного правительства. Архитектура предприятия — это основа стратегического планирования, которая связывает и согласовывает ИКТ с бизнес-функциями, которые они поддерживают. Создание EA на национальном уровне началось с федерального правительства США, и многие страны в настоящее время создают и применяют национальные EA (Christiansen and Gotze, 2007). Например, правительство Дании описывает свою EA как «общую структуру, которая обеспечивает общую согласованность между ИТ-системами государственного сектора, в то же время позволяет оптимизировать системы с точки зрения местных потребностей. Это общая рамочная основа, направленная на повышение качества, оптимизацию ресурсов и снижение затрат».

Архитектура федерального предприятия (англ. Federal Enterprise Architecture, FEA) — это EA федерального правительства США. FEAF версии 2.0 является последней принятой версией, включающей CPM и 6 эталонных моделей. Исходя из этого, управление EA ведомства входит в обязанности CIO этого ведомства. В Корее также действует общеправительственная EA, опираясь на опыт FEA в США. Поскольку EA охватывает бизнес-процессы, данные, услуги и технологии всей организации, многие страны устанавливают политики IF для обеспечения их совместимости. В Корее существует эталонная технологическая модель (TRM) общеправительственной EA, структура управления функциональной совместимостью.

II.2.3.4 Стандартная структура электронного правительства

Стандартная структура электронного правительства представляет собой инфраструктурную среду для реализации прикладного программного обеспечения (ПО) и обеспечивает базовые функции во время выполнения прикладного ПО. Целью стандартной структуры электронного правительства является повышение качества услуг электронного правительства, эффективности инвестиций в ИТ, а также стандартизация и возможность повторного использования прикладных программных приложений посредством создания и применения стандарта платформы разработки.

II.2.4. Международные исследования (ООН, ВБ, ОЭСР) и стандарты совместимости

Многие международные организации публикуют аналитические отчеты о текущем состоянии электронного правительства в каждой стране. Международные организации рассылают анкеты для определения ситуации по цифровизации, включая политику и ситуацию по обеспечению интероперабельности, в участвующих странах и анализируют их ответы, которые представляются в форме [ежегодного] отчета. В этом разделе кратко представлены результаты индексов по вопросам интероперабельности.

[11] ПРООН. 2007. Руководство по совместимости электронного правительства. https://www.unapcict.org/sites/default/files/2019-01/e-Government%20Interoperability%20-%20Guide.pdf

II.2.4.1 ООН (EGDI)

Индекс развития электронного правительства (EGDI) представляет положение по развитию электронного правительства в государствах-членах Организации Объединенных Наций[12]. Наряду с оценкой моделей развития веб-сайтов в стране, индекс развития электронного правительства включает характеристики доступа, такие как уровень инфраструктуры и уровень образования, чтобы отразить то, как страна использует информационные технологии для содействия доступу и вовлечению населения. EGDI представляет собой комплексный показатель трех важных аспектов электронного правительства, а именно: предоставление онлайн-услуг, телекоммуникации и человеческий потенциал.

Согласно отчету ООН, страны, лидирующие в развитии электронного правительства имеют специализированные законы или нормы, касающиеся цифровых закупок, цифровой идентификации и цифровых подписей, а также нормативно-правовые рамки, регулирующие доступ к информации, такой как обмен данными, взаимодействие между государственными учреждениями и государственные расходы[13].

II.2.4.2 Всемирный банк (GTMI)

Индекс зрелости государственных технологий (GTMI) был разработан в рамках Инициативы GovTech для определения степени зрелости государственных технологий в четырех основных сферах[14], а также для оказания помощи специалистам-практикам в разработке новых проектов цифровой трансформации. Версия GTMI 2022 года представляет собой простое среднее значение нормализованных оценок четырех элементов[1]:

- ***CGSI:*** Индекс основных государственных систем (17 показателей) отражает ключевые аспекты общегосударственного подхода, включая правительственное облако, системы совместимости и другие платформы.
- ***PSDI:*** Индекс предоставления государственных услуг (9 показателей) измеряет зрелость онлайн-порталов государственных услуг с упором на дизайн, ориентированный на граждан, и универсальную доступность.

---

[12] ООН. База знаний ООН по электронному правительству – Индекс развития электронного правительства (EGDI). https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index
ООН. Исследование по электронному правительству за 2022 год. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2022 .

[13] Исследование ООН включает следующие вопросы, связанные с совместимостью: (1) Существуют ли какие-либо законы или правила, касающиеся национального управления данными, включая совместное использование данных/обмен/взаимодействие между государственными учреждениями? (Взаимодействие данных); (2) Существует ли национальная стратегия электронного правительства или эквивалентная стратегия? (Может включать стратегии совместимости); (3) Предусматривает ли правительство конкретные меры для обеспечения полноценного подключения/доступа к услугам электронного правительства для женщин и/или других уязвимых групп? (Может включать критерии совместимости, включая доступность).

[14] (1) Поддержка основных государственных систем; (2) Улучшение предоставления услуг; (3) Активизация участия граждан; и (4) содействие развитию государственных технологий.

[1] Всемирный банк (ВБ). Государственные технологии: люди прежде всего. https://www.worldbank.org/en/programs/govtech/gtmi

- ***DCEI:*** Индекс вовлеченности граждан (6 показателей) измеряет аспекты платформ участия общественности, механизмов обратной связи от граждан, открытых данных и открытых правительственных порталов.
- ***GTEI:*** Индекс поддержки государственных технологий (16 показателей) отражает стратегию, институты, законы и нормативные акты, а также цифровые навыки, а также инновационную политику и программы для развития государственных технологий.

Таблица 5: Исследование ВБ GTMI: Основная государственная система, 1_3. GIF

Число	Вопрос
1_3	Существуют ли государственные рамки/стандарт обеспечения интероперабельности (GIF)?
1_3.1	I-3.1 Название отчета GIF.
1_3.2	Отчет GIF/проект URL.
1_3.3	GIF был внедрен/будет введен в (году).
1_3.4	Текущий статус GIF.
1_3.5	Сфера применения > Есть ли общий GIF?
1_3.6	Существует ли система качества данных?
1_3.7	Существует ли система мониторинга работоспособности государственных информационных систем?
1_3.8	Существуют ли рекомендации по замене устаревших государственных информационных систем?
1_3.9	Мониторинг и публикация использования GIF, соблюдения требований и преимуществ?
1_3.9.1	Если да > Подтверждающий документ (отчет/URL).

Согласно исследованию в общей сложности 85 стран (43%) заявили о наличии у них государственных рамок обеспечения интероперабельности (GIF), а 40 стран сообщили, что такие рамки широко ими используются. Несмотря на то, что результаты GTMI 2022 года свидетельствуют об актуальности интероперабельности, являющейся ключевым аспектом развития государственных технологий, необходимы значительные инвестиции для ее внедрения в подавляющем большинстве опрошенных стран.

II.2.4. 3 ОЭСР (DGI)

Индекс цифрового правительства ОЭСР (DGI) оценивает полноту стратегий и инициатив цифрового правительства, оценивая наличие общегосударственного подхода к внедрению цифровых технологий и использованию данных в центральных и федеральных организациях государственного сектора.[15]

Оценка основана на шести аспектах Руководства ОЭСР по политике цифрового правительства: (1) цифровое по замыслу; (2) государственный сектор, управляемый данными; (3) правительство как платформа; (4) открытое по умолчанию; (5) управляемое пользователем; и 6) инициативность. DGI является составным индексом, со значением от 0 до 1, где 1 указывает на самую высокий уровень зрелости цифрового правительства, а 0 указывает на низкий и/или фрагментированный прогресс организаций. Последняя

[15] ОЭСР. Going Digital Toolkit – Индекс цифрового правительства (DGI) https://goingdigital.oecd.org/en/indicator/58

анкета состоит в общей сложности из шести частей; [16] все части включают вопросы, связанные с интероперабельностью.

II.3 Сравнение различных стандартов e-GIF

Во многих странах разработаны рамочные стандарты, такие как e-GIF, для обеспечения совместимости, но также продвигаются и другие виды политики обеспечения совместимости. Ниже сравним e-GIF с четырьмя другими вариантами, а подробности каждого варианта объяснены в разделе «Практические примеры».

- ***EIF.*** Если e-GIF предназначен для обеспечения совместимости внутри стран, то EIF представляет собой рамочный стандарт ЕС, обеспечивающий совместимость между странами.
- ***X-Road в Эстонии.*** X-Road представляет собой уровень для обмена данными в Эстонии и реализован как реальная информационная система. X-Road является основой для обеспечения взаимодействия между подключенными системами путем связывания информационных систем согласно предложенным протоколам и интерфейсам.
- ***Архитектура предприятия (EA).*** В США Директор по информационным технологиям (CIO) государственного учреждения организует и управляет EA учреждения как основой для разработки и эксплуатации информационной системы. EA представляет рекомендации по обеспечению совместимости с помощью шести субархитектур и эталонных моделей для каждой архитектуры.
- ***Система электронного правительства Кореи.*** Эта система представляет собой стандартизированную среду разработки, предназначенную для решения проблемы отсутствия совместимости при объединении или улучшении информационных систем, созданных из-за различных сред разработки при продвижении проектов информатизации и разработке информационных систем. Она была создана для обеспечения совместимости и взаимодействия уже на этапе разработки информационных систем и программного обеспечения.

Основные различия между e-GIF и другими платформами:

- EIF и X-Road расширяются для обеспечения совместимости между странами.
- США стремятся к функциональной совместимости с точки зрения архитектуры, а также есть случаи фактической стандартизации в других странах и частном секторе.
- Рамочный стандарт электронного правительства обеспечивает функциональную совместимость за счет применения общих компонентов на этапе разработки.
- Политика правительства США, основанная на EA, по-видимому, была первой общегосударственной политикой обеспечения совместимости (Управление управления и бюджета, OMB 97-16). Однако e-GIF, разработанный в Великобритании, применялся во многих странах быстрее, чем распространялись политики совместимости на основе EA.

[16] Специальная часть по постпандемической оценке COVID-19; (1) Управление цифровым правительством; (2) Потенциал государственного сектора для цифрового правительства; (3) Государственный сектор, управляемый данными; (IV) Открытые государственные данные – из Обзора открытых государственных данных 5.0; (5) Разработка и предоставление услуг в эпоху цифровых технологий.

Table 6: Comparison of interoperability framework policy

Рамочная политика	Ключевые компоненты	Сильные стороны	Недостатки	Лучшие примеры использования
e-GIF	• электронная GMS. • Каталог государственных стандартов данных. • XML-схемы. • Каталог технических стандартов.	• Прагматичный подход на базе Интернета для снижения затрат и рисков. • Используется многими странами в качестве ведущего примера политики обеспечения совместимости.	• Пересмотры не выпускались после 2005 года.	• Распространен на более чем 30 стран и связан с EIF.
EIF	• Одна концептуальная модель. • Четыре уровня совместимости. • 12 основополагающих принципов. • 47 рекомендаций.	• Расширение совместимости между странами.	• Требуется детальное подключение и применение с учетом особенностей каждой страны.	• Непрерывные улучшения со стороны экспертной группы ЕС.
X-Road (x-tee)	• (Архитектура X-ROAD) • Центральный сервис. • Сервис безопасности. • Информационная система. • Добавление отметки времени (TSA). • Центр сертификации (ЦС).	• (ВЛАДЕЛЬЦЫ ЭКОСИСТЕМЫ X-ROAD) Централизованное управление; Масштабируемость; Доверие и прозрачность; Возможности сотрудничества; Экономия затрат. • (УЧАСТНИКИ ЭКОСИСТЕМЫ X-ROAD) Безопасный обмен данными; совместимость; Упрощенная интеграция; Доступ к источникам данных; Повышенная эффективность. • (ПРЕИМУЩЕСТВА ДЛЯ КОМПАНИЙ) Рыночный потенциал; Конкурентное преимущество; Возможность повторного использования и масштабируемость; Экономия затрат и эффективность; Поддержка и ресурсы сообщества; Партнерская программа X-Road Technology.	• При переходе от устаревшей системы или среды разработки необходимо учитывать множество факторов.	• Содействие межстрановому сотрудничеству с Финляндией и усилия по его распространению на многие страны.
EA (см. FEA)	(Архитектура предприятия) • Базовая архитектура. • Целевая архитектура. • План перехода. (структура федеральной архитектуры предприятия)	• Обеспечение общего подхода к приобретению ИТ в федеральном правительстве США. • Облегчение обмена информацией и ресурсами между федеральными агентствами. • Сокращение расходов и улучшение услуг для граждан.	• Трудности в достижении желаемых целей, поскольку требуется обширное и постоянное управление.	• Многие страны применяют его в своих условиях, и есть много примеров и

Рамочная политика	Ключевые компоненты	Сильные стороны	Недостатки	Лучшие примеры использования
	• Методология совместного планирования. • Общий подход Эталонная модель.			инструментов в частном секторе (TOGAF и т.д.).
e-Gov. S/F	(Архитектура системы электронного правительства) • Среда выполнения (Lite). • Среда разработки. • Управленческая среда. • Операционная среда. • Общие компоненты.	• Улучшение качества, сопровождающееся повышением продуктивности разработки. • Максимизация возможности повторного использования и взаимодействия. • Повышение уровня стандартизации информационных услуг.	• Поскольку основное внимание уделяется обеспечению совместимости в конкретных областях (развития), необходимы также политики и в других областях, таких как обмен данными. • Требуется совместимость с другими гражданскими системами.	• Представление модели экосистемы на уровне структуры разработки строительных блоков (общих компонентов). • Применение стандартной структуры электронного правительства к 6 359 проектам общественной информатизации.

II.4 Объяснение различных рамок обеспечения совместимости

В этом разделе подробно рассматриваются конкретные детали различных рамочных документов, кратко представленных ранее.

II.4.1 Европейский свод требований по совместимости (EIF)

В 2017 году ЕС объявил о новом Европейском своде требований по совместимости, направленном на обеспечение бесперебойных услуг и потоков данных для государственных органов стран ЕС. Европейский свод требований по совместимости представляет собой общепринятый подход к оказанию европейских государственных услуг на совместимой основе. Он определяет основные руководящие принципы совместимости в форме общих принципов, моделей и рекомендаций.

Целями EIF являются:

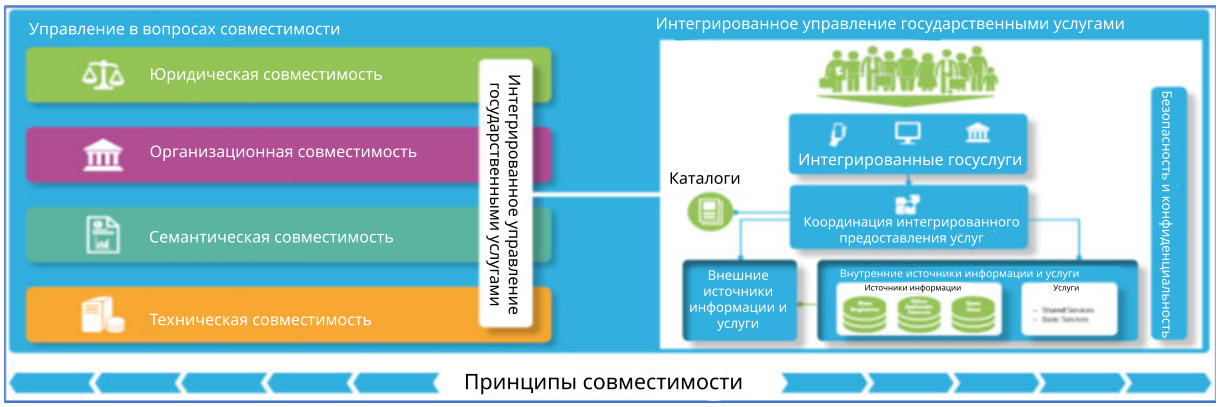
- Мотивирование государственных органов стран ЕС в их усилиях по разработке и оказанию бесперебойных европейских государственных услуг предприятиям и гражданам, которые, насколько это возможно, являются по умолчанию цифровыми, трансграничными и открытыми;
- Предоставление руководящих указаний государственным органам по разработке и обновлению национальных рамок совместимости (NIF) или национальной политики, стратегий и руководящих принципов, способствующих совместимости;
- Внесение вклада в создание Единого цифрового рынка (DSM) путем содействия трансграничной и межотраслевой совместимости для предоставления европейских государственных услуг.

EIF был пересмотрен с целью (1) приведения его в соответствие с изменениями в политике; (2) расширения и приведение в соответствие с новыми тенденциями; и (3) акцентирования внимания на реализацию EIF.

Элементами EIF являются одна концептуальная модель, четыре уровня совместимости, 12 основных принципов и 47 рекомендаций. Содержание и структура EIF представлены ниже:

- ***Глава 2.*** Представлен набор принципов, предназначенных для установления общих правил совместимости;
- ***Глава 3.*** Представлена многоуровневая модель совместимости, которая организует по уровням различные аспекты совместимости, которые необходимо учитывать при разработке европейских государственных услуг;
- ***Глава 4.*** Описана концептуальная модель совместимых государственных услуг. Модель соответствует принципам совместимости и продвигает идею «совместимости по замыслу» как стандартного подхода к проектированию и функционированию европейских государственных услуг;
- ***Глава 5.*** Представлен обзор и основные элементы EIF.

Рис. 2: Пересмотренная концептуальная модель EIF



Вставка 4: Пример рекомендации

Рекомендация 39
Сопоставьте каждый базовый реестр с соответствующими метаданными, включая описание его содержания, гарантированного качества услуг и обязанности, тип хранимых в нем основных данных, условия доступа и соответствующие лицензии, терминологию, глоссарий и информацию о любых основных данных, которые он использует, из других базовых реестров.

II.4.2 X-Road (X-tee)

X-Road представляет собой слой обмена данными с открытым исходным кодом, которое позволяет организациям обмениваться информацией через Интернет. X-Road — это централизованно управляемый распределенный слой обмена данными между информационными системами, который обеспечивает стандартизированный и безопасный способ производства и потребления услуг. X-Road основан на распределенной архитектуре и обеспечивает конфиденциальность, целостность и совместимость между сторонами обмена данными. Он предоставляет встроенную модель организационного управления, которая поддерживает создание и эксплуатацию общенациональной экосистемы X-Road. X-Road является основой электронной Эстонии, невидимой, но очень важной, поскольку она позволяет различным государственным и частным информационным системам электронных услуг объединяться и гармонично функционировать. Первая версия X-Road была выпущена в Эстонии в 2001 году. Техническая реализация X-Road развивалась и менялась с годами, но основная концепция с самого начала остается прежней.

Эстонская среда X-Road «X-tee» (национальный слой обмена данными Эстонии), откуда и произошло название X-Road, включает в себя полный спектр услуг для широкой публики, и поскольку каждая услуга имеет свою собственную информационную систему, все они полагаются на X-Road. Чтобы обеспечить безопасную передачу, все исходящие данные снабжаются цифровой подписью и шифруются, а все входящие данные проверяются на подлинность и регистрируются.

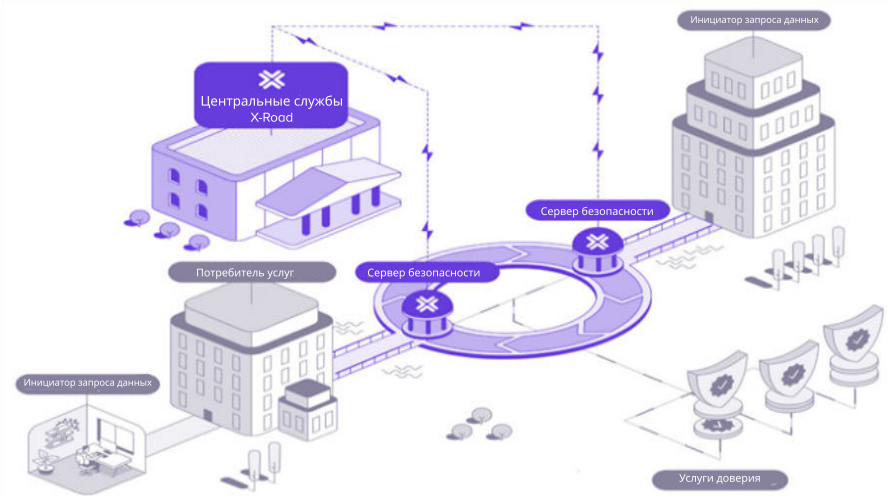
X-Road объединяет различные информационные системы, которые могут включать в себя множество сервисов. Он превратился в инструмент, который также может

обращаться в несколько информационных систем, передавать большие наборы данных и выполнять поиск в нескольких информационных системах одновременно. X-Road был разработан с учетом роста, поэтому его можно масштабировать по мере появления в сети новых электронных услуг и платформ. X-Road является цифровым общественным благом, подтвержденным Альянсом цифровых общественных благ, выпущенным по лицензии MIT с открытым исходным кодом и доступное бесплатно.

Вставка 5: Особенности X-Road

- Управление адресами
- Маршрутизация сообщений
- Управление правами доступа
- Проверка подлинности на уровне организации
- Проверка подлинности на уровне машины
- Шифрование на транспортном уровне
- Отметки времени
- Цифровая подпись сообщений.
- Ведение журнала событий
- Обнаружение и коррекция ошибок.

Рис. 3: Архитектура X-Road



Технически экосистема X-Road состоит из центральных служб, серверов безопасности, информационных систем, TSA и CA.

- ***Центральные службы:*** центральные службы состоят из центрального сервера и прокси-сервера конфигурации. Центральный сервер содержит реестр участников X-Road и их серверов безопасности. Кроме того, Центральный сервер содержит политику безопасности X-Road, включающую список доверенных центров сертификации, список доверенных центров регистрации времени и параметры конфигурации. И реестр участников, и политика безопасности доступны серверам безопасности по протоколу HTTP.

- ***Серверы безопасности:*** серверы безопасности являются посредниками при запросах и ответах между информационными системами. Серверы безопасности инкапсулируют аспекты безопасности инфраструктуры X-Road: управление ключами для подписи и проверки подлинности, отправка сообщений по

- защищенному каналу, создание проверочного значения для сообщений с цифровыми подписями, метки времени и ведение журнала событий.

- ***Информационные системы:*** информационные системы производят и/или потребляют услуги через X-Road и принадлежат участнику X-Road. X-Road поддерживает использование и создание услуг как REST (передача состояния представления), так и по протоколу SOAP. Однако X-Road не обеспечивает автоматическое преобразование между различными типами сообщений и услуг.

- ***Службы отметок времени (TSA):*** все сообщения, отправляемые через X-Road, имеют отметку времени и регистрируются сервером безопасности. Целью отметки времени является подтверждение существования элементов данных в определенный момент времени. TSA предоставляет сервис отметки времени, который сервер безопасности использует для отметки времени во всех входящих/исходящих запросах/ответах. Можно использовать только доверенные TSA, определенные на центральном сервере.

- ***Центр сертификации (ЦС):*** центр сертификации (ЦС) выдает сертификаты серверам безопасности (сертификаты аутентификации) и организациям-членам X-Road (сертификаты проверки подлинности). Сертификаты проверки подлинности используются для защиты соединения между двумя серверами безопасности. Для цифровой подписи сообщений, отправляемых участниками X-Road, используются сертификаты подписи. Можно использовать только сертификаты, выданные доверенными центрами сертификации, которые определены на центральном сервере.

Сегодня X-Road реализуется более чем в 20 странах мира. X-Road обеспечивает встроенную поддержку трансграничного обмена данными посредством интеграции, что означает объединение двух экосистем X-Road. Члены интегрированных экосистем могут публиковать и использовать услуги друг с другом, как если бы они были членами одной экосистемы[17].

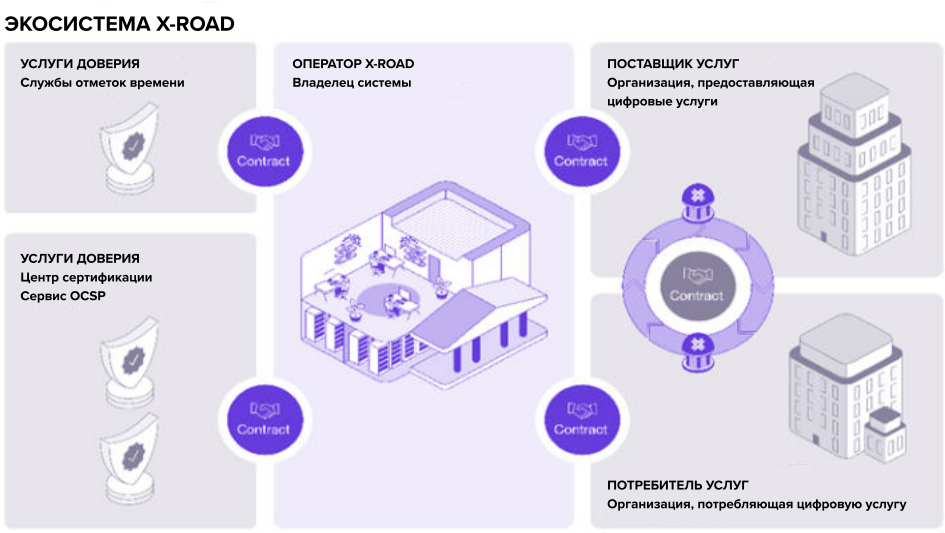
Эстония и Финляндия совместно учредили Институт решений по взаимодействию стран Северной Европы (NIIS), некоммерческую ассоциацию, которая обеспечивает разработку и стратегическое управление X-Road® и другими трансграничными решениями для инфраструктуры цифрового правительства. Ее миссия состоит в разработке решений электронного управления, начиная с X-Road. NIIS отвечает за развитие ядра X-Road и поддержку его участников[18]. X-Road используется по всей стране на уровне обмена данными X-tee в Эстонии и в сервисе уровня обмена данными Suomi.fi в Финляндии. X-Road выпускается по лицензии MIT с открытым исходным кодом и доступен бесплатно для любого человека или организации.

---

[17] Две экосистемы X-Road могут быть объединены, т.е. интегрированы в отношения один к одному между двумя экосистемами. Интеграция обеспечивает простой и безопасный трансграничный обмен данными между государствами-членами с помощью X-Road, а члены интегрированных экосистем могут публиковать и использовать услуги друг с другом, как если бы они были членами одной экосистемы. В X-Road применяются такие технологии, как Linux, Java, SOAP, REST и PKI.

[18] Институт решений по взаимодействию стран Северной Европы. Является ли X-Road космической технологией данных? NIIS. https://www.niis.org/blog/2023/6/21/is-x-road-a-data-space-technology ; Архитектура X-Road®, https://x-road.global/architecture

Рис. 4. Экосистема X-Road.



II.4.3 Рамочная структура архитектуры федерального предприятия (FEAF)

В США в соответствии с Законом об электронном правительстве администраторы государственных ведомств контролируют развитие архитектуры предприятия внутри и между ведомствами. С юридической точки зрения архитектура предприятия означает: (1) базу стратегических информационных активов, определяющую миссию; (2) информацию, необходимую для выполнения миссии; (3) навыки, необходимые для выполнения миссии; и (4) переходный процесс для внедрения новых технологий, отвечающих меняющимся потребностям миссий. Она включает в себя (1) базовую архитектуру; (2) целевую архитектуру; и (3) планирование последовательности. Рамочная структура архитектуры федерального предприятия (FEAF) — это руководство по поддержке разработки и эксплуатации EA во всех государственных ведомствах США. FEAF v2 описывает набор инструментов, помогающих реализовывать общий подход, и включает CRM, CPM и артефакты [19].

II.4.3.1 Консолидированная эталонная модель

В ее основе лежит Консолидированная эталонная модель (CRM), которая предоставляет Административно-бюджетному управлению и федеральным ведомствам общий язык и структуру для описания и анализа инвестиций. Она состоит из набора взаимосвязанных «эталонных моделей», которые описывают шесть областей субархитектуры: (1) Стратегия; (2) Бизнес; (3) Данные; (4) Приложения; (5) Инфраструктура; (6) Безопасность.

Они предназначены для облегчения межведомственного анализа и выявления дублирующих инвестиций, пробелов и возможностей для сотрудничества внутри ведомств и между ними. Кроме того, применяя все шесть эталонных моделей, ведомства могут установить связь между стратегическими целями на самом высоком организационном уровне и инфраструктурой программного и аппаратного обеспечения, обеспечивающей достижение этих целей. В совокупности эталонные модели составляют основу для описания важных элементов деятельности федеральных ведомств единым и последовательным образом.

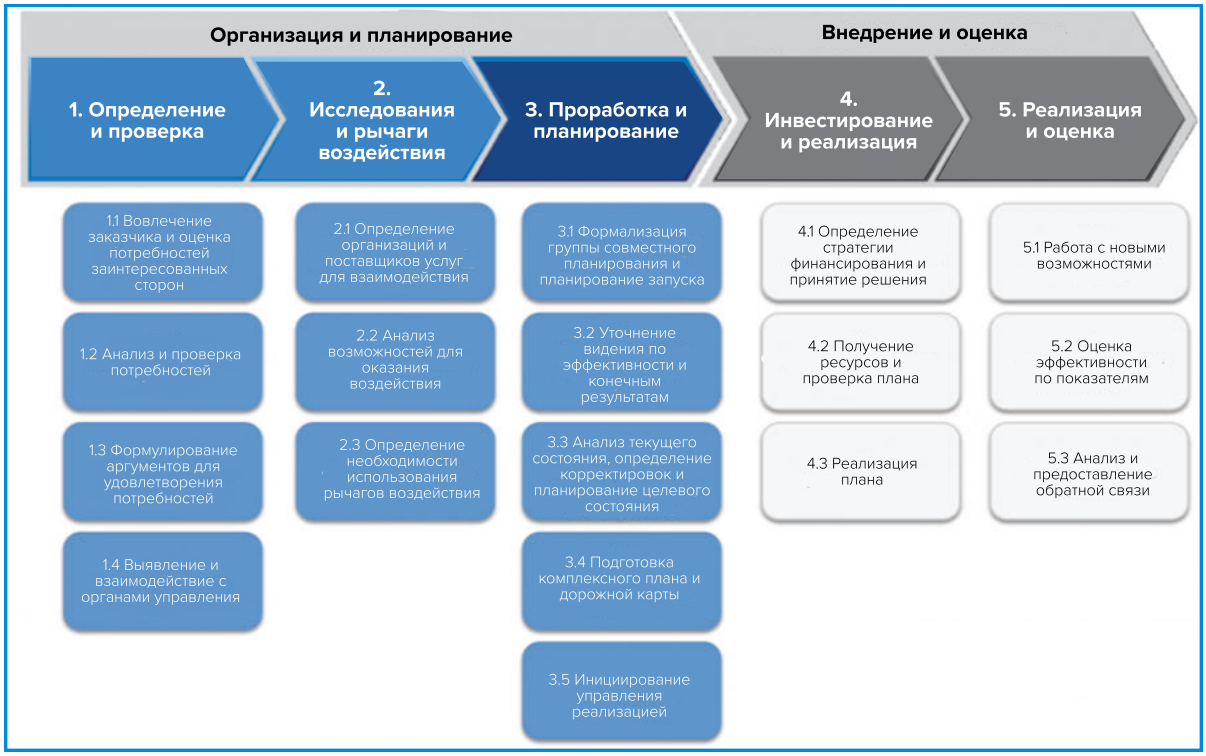
[19] Рамочная структура архитектуры федерального предприятия, версия 2. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf

Рис. 5. Консолидированная эталонная модель.

II.4.3.2 Методология совместного планирования

Настоящая ценность для ведомства в разработке архитектуры предприятия состоит в том, чтобы облегчить планирование будущего таким образом, чтобы трансформировать государственный аппарат и сделать его более эффективным. Ведомство может использовать процесс EA для описания предприятия в его нынешнем виде и определения того, как предприятие должно выглядеть в будущем, чтобы оно могло планировать переход от текущего состояния к будущему. Методология совместного планирования содержит шаги, которые специалисты по планированию могут использовать на протяжении всего процесса планирования, чтобы конкретизировать стратегию перехода, которая позволит будущему состоянию стать реальностью. Это простой, повторяемый процесс, состоящий из интегрированного междисциплинарного анализа, в котором участвуют инициаторы, заинтересованные стороны, специалисты по планированию и исполнители.

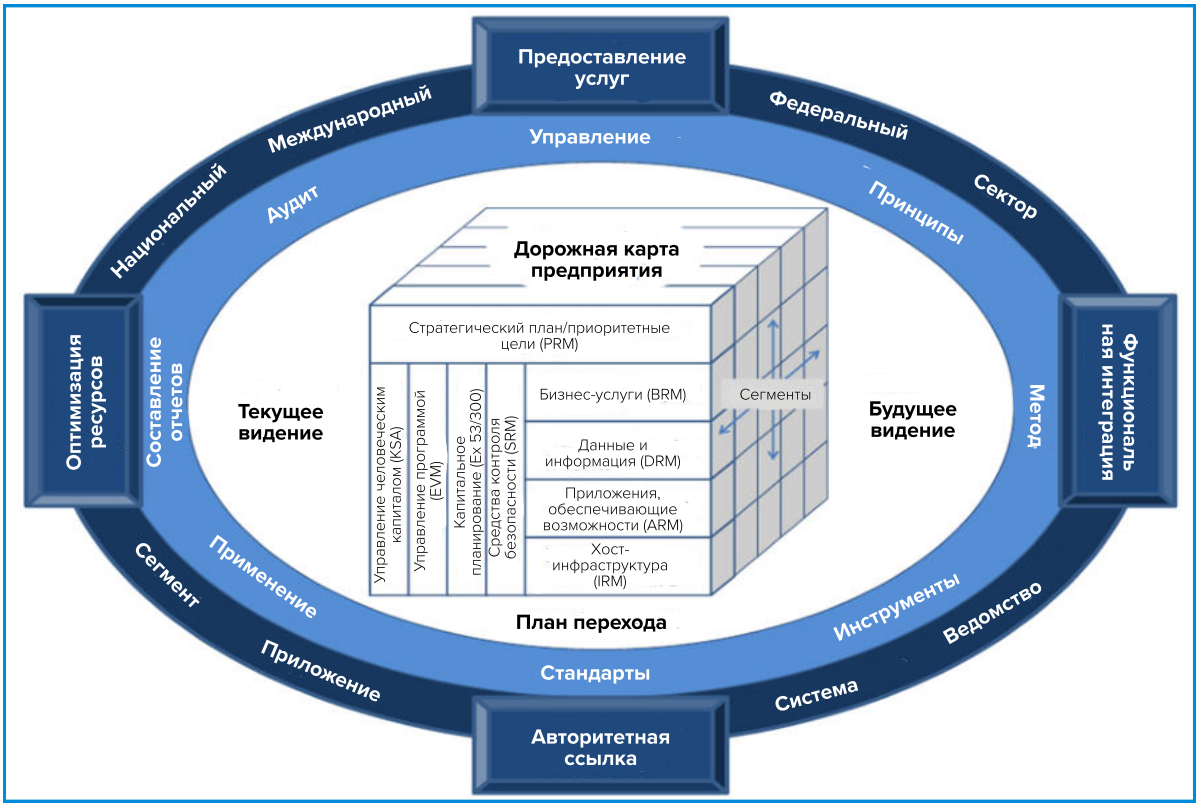
Рис. 6. Методология совместного планирования.



II.4.3. 3 артефакта

Ведомство подготовит Дорожную карту предприятия, чтобы задокументировать в укрупненном виде текущее и будущее состояние архитектуры, и представит план перехода, т.е. то, как ведомство будет двигаться от настоящего к будущему эффективным и результативным образом. Дорожная карта предприятия объединяет артефакты, разработанные для EA, как в текущей, так и будущей версии, с планом, разработанным с помощью методологии совместного планирования. Это обеспечивает осведомленность, наглядность и прозрачность внутри организации, что облегчает межорганизационное планирование и сотрудничество. Дорожная карта сопоставляет стратегию с проектами и бюджетом и помогает выявить разрывы между инвестициями и исполнением, а также зависимости и риски между проектами.

Рис. 7: Артефакты EA



В общем подходе к архитектуре федерального предприятия есть шесть областей субархитектуры: (1) Стратегия; (2) Бизнес услуги; (3) Данные и информация; (4) Приложения; (5) Хост-инфраструктура; и (6) Безопасность. Эти шесть областей субархитектуры определяют виды анализа и моделирования, необходимые для удовлетворения требований заинтересованных сторон.

Основываясь на передовом опыте EA, в «Общем подходе к архитектуре федерального предприятия» указан один обязательный артефакт основной документации для каждой из шести областей на высоком уровне субархитектуры.

Таблица 7: Основной документ

Область субархитектуры	Необходимый основной артефакт
Стратегия	Обзорная схема концепции
Бизнес	Укрупненная диаграмма процесса
Данные	Укрупненная логическая модель данных
Приложения	Схема интерфейса приложений
Инфраструктура	Укрупненная схема сети
Безопасность	Контрольный список

В целом, Рамочная структура архитектуры федерального предприятия (версия 2) помогает ускорить трансформацию деятельности ведомств и внедрение новых технологий, предоставляя инструменты стандартизации, анализа и отчетности, дорожную карту предприятия и повторяемый метод проекта архитектуры, который является более гибким и полезным и позволит создавать более достоверную информацию для внутриведомственного и межведомственного планирования, принятия решений и управления.

II.4.4.5 Стандартная структура электронного правительства

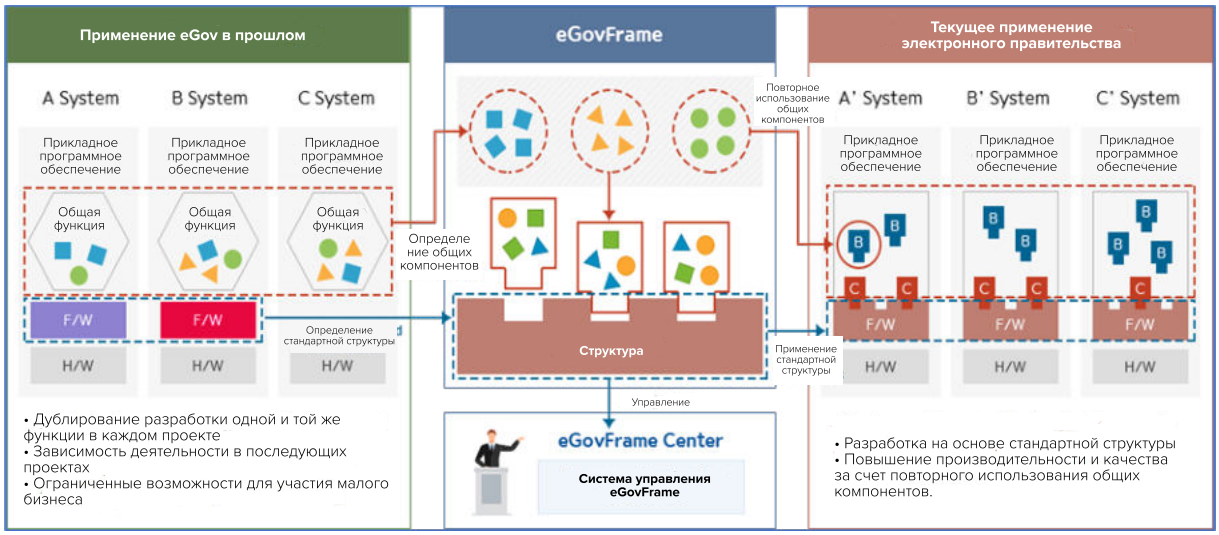
Стандартная структура электронного правительства представляет собой стандартизированный рамочный документ для разработки ИТ-проектов на разных платформах в государственном секторе в Корее.

В существующей системе электронного правительства есть множество проблем, поскольку каждая отдельная прикладная система использует различные виды и версии инфраструктур. Среды разработки, используемые в существующей системе электронного правительства, трудно поддерживать без технической поддержки поставщиков, поскольку они предоставляются в виде модулей по принципу «черного ящика» и, таким образом, зависят от конкретного поставщика.

Стандартизация методологии электронного правительства устраняет техническую зависимость от платформ разработки, принадлежащих поставщикам, способствует стандартизации и, таким образом, повышает качество и возможность повторного использования прикладных программных комплексов. Это также повышает эффективность инвестиций за счет унификации обслуживания структуры развития.

Стандартная структура электронного правительства представляет собой инфраструктурную среду для реализации прикладного ПО и предоставляет базовые функции во время выполнения прикладного ПО. Стандартная структура электронного правительства имеет целью повысить качество услуг электронного правительства, эффективность инвестиций в ИТ, а также стандартизировать и обеспечить возможность повторного использования прикладного ПО посредством создания и применения стандарта платформы разработки. В Стандартной структуре электронного правительства используется лицензия Apache версии 2.0, при этом другие ПО с открытым исходным кодом, используемые в Стандартной структуре, сохраняют применимую политику лицензирования.

Рис. 8: Стандартизация структуры электронного правительства



Функции

Стандартная структура электронного правительства имеет следующие функции для достижения своей цели по повышению функциональной совместимости и возможности повторного использования национальных информационных систем.

- Соответствует открытым стандартам.
- Интегрируется с коммерческими решениями.
- Ориентирована на стандартизацию в национальном масштабе.
- Гибкая для того, чтобы позволять работать с новейшими технологиями.
- Обеспечивает простую в использовании и многофункциональную среду.

Преимущества

Стандартная структура электронного правительства повышает продуктивность разработки и возможность повторного использования компонентов в прикладных системах, предоставляя стандартизированную инфраструктуру, увеличивает функциональную совместимость и способствует стандартизации прикладных программных средств посредством стандартов интерфейса.

- Повышение продуктивности разработки.
- Увеличение возможности повторного использования прикладных систем электронного правительства.
- Повышение совместимости систем электронного правительства.
- Стандартизация прикладных систем электронного правительства.
- Продвижение использования ПО с открытым исходным кодом.
- Повышение конкурентоспособности малых и средних поставщиков ПО.

Вставка 6: Видение, цели и стратегии Стандартной структуры электронного правительства

Видение

Повышение качества услуг электронного правительства и эффективности инвестиций в ИКТ.

Цели

- Повторное использование общих функций
- Повышение совместимости
- Отражение последних тенденций в области ИКТ
- Устранение зависимости от поставщиков
- Повышение конкурентоспособности МСБ.

Стратегии

- Стандартизация
- Открытость
- Сообщество.

Состав

Стандартная структура электронного правительства состоит из 8 уровней сервиса, общих компонентов (шаблонов), среды выполнения, среды эксплуатации, среды разработки и среды администрирования. Стандартная структура, состоящая из среды выполнения, среды разработки, среды управления и операционной среды и Общих компонентов, представляют архитектуру приложений для разработки систем веб-приложений.

Рис. 9: Структура стандартной структуры электронного правительства

Таблица 8: Архитектура стандартной структуры электронного правительства

Компонент	Функции и роли
Среда выполнения	Среда выполнения является основой программных приложений и обеспечивает базовую функциональность, необходимую для запуска корпоративного приложения. Среда выполнения стандартной структуры электронного правительства состоит из 8 уровней сервисов и предоставляет 39 сервисов.
Среда разработки	В качестве базового модуля, на котором работают веб-приложения, состоящего из 5 уровней, таких как обработка экрана, обработка бизнес-логики, обработка данных, обработка интеграции и общая основа. В качестве набора инструментов для легкой разработки прикладных программ на основе инструмента разработки экранов, инструмента разработки компонентов, инструмента разработки данных, инструмента автоматизации тестирования, инструмента проверки кода, инструмента создания шаблонного проекта, инструмента общего компонента, Инструмента настройки композиции разработки, Инструмента управления средой сервера, Инструмента генерации стандартного мобильного исходного кода, Набора инструментов для создания проектов мобильных шаблонов, Набора мобильных инструментов общего компонента, Набора инструментов кастомизированной мобильной разработки, Среды разработки сервера (Windows, Unix и т. д.) и набора инструментов для установки.
Операционная среда	Система для различных операций стандартной платформы, таких как мониторинг прикладных программ, работающих в среде выполнения, управление различными сбоями системы и т.д.
Среда управления	Система для различных операций стандартной платформы, таких как мониторинг прикладных программ, работающих в среде выполнения, управление различными сбоями системы и т.д.
Общий компонент	Система для различных операций стандартной платформы, таких как мониторинг прикладных программ, работающих в среде выполнения, управление различными сбоями системы и т.д.

II.5 Заключение

В этой публикации представлены разные примеры методологий архитектуры взаимодействия электронного правительства в Великобритании, ЕС, США и Корее. Далее резюмируем их эффект по некоторым важным элементам.

II.5.1 Управление

Как видно из исследований, проводимых международными организациями, обеспечение совместимости требует обширной политики с различных точек зрения в дополнение к техническим стандартам и спецификациям. Например, связь с национальной политикой, создание базового плана, учет удобства для общественности, такого как доступность, создание среды для применения функциональной совместимости и т.д.

В соответствии с этой необходимостью бывают случаи, когда вместо единой политики обеспечения совместимости применяется несколько политик или корректируется сфера их применения. Например, большинство архитектур взаимодействия электронного правительства (e-GIF) предоставляются в форме стандартов или руководств. Следовательно, чтобы обеспечить соответствие, эти политики должны быть связаны с такими процедурами, как проектирование, тестирование и аудит. В случае Кореи необходимость соответствия e-GIF указывается в техническом задании на подготовку проекта информационной системы, и выполнение этого условия проверяется в конце реализации проекта. В случае с США создание архитектуры предприятия и обеспечение соблюдения стандартов входит в обязанности директора по информационным технологиям. Таким образом, чтобы улучшить функциональную совместимость по всей стране, необходимо создать правовую и институциональную систему управления для эффективной реализации политики обеспечения совместимости.

II.5.2 Выбор подходящей модели e-GIF.

Уровень и направление политики обеспечения совместимости различаются в зависимости от условий и особенностей каждой страны. Поэтому предпринимается все больше усилий по улучшению совместимости, чтобы соответствовать реалиям каждой страны, опираясь на опыт других стран по таким политикам и системам обеспечения совместимости. Эти изменения происходят по-разному, например, за пределами страны или из-за ограничений в более конкретных стандартах. Следовательно, при выборе рамочного документа по совместимости необходимо учитывать уровень развития электронного правительства, состояние строительства инфраструктуры и объем целей, требующих совместимости.

II.5.3 Выбор подходящей технологии

В e-GIF должна быть выбрана технология, подходящая для среды государственной информационной системы, и должны быть представлены принципы этого процесса. В последние годы, с распространением Интернета, в большей степени преобладают политики совместимости, ориентированные на данные, а не на улучшение совместимости в отношении физических сред, таких как сети и серверы. Кроме того, скорость изменений в ИТ очень высока, поэтому необходимо создать систему мониторинга и выбора технологий и стандартов.

II.6 Список литературы

- CS Transform. e-Government Interoperability A comparative analysis of 30 countries. (2010). https://lists.oasis-open.org/archives/tgf/201101/pdf00010.pdf
- Ana Lisboa, Delfina Soares (2014), E-Government interoperability frameworks: a worldwide inventory, https://doi.org/10.1016/j.protcy.2014.10.012
- National Archives. (2010). Cabinet Office. Archived e-GIF Published Documents - Title: Interoperability News. https://webarchive.nationalarchives.gov.uk/ukgwa/20111205213424/http://interim.cabinetoffice.gov.uk/govtalk/archive/policy_documents_1_of_1/e-gif/e-gif_published_documents/interoperability_news.aspx
- Ministry of the Interior and Safety, NIA. E-GOV Frame Portal https://www.egovframe.go.kr/eng/sub.do?menuNo=7
- Ministry of the Interior and Safety, NIA. E-GOV Frame Portal. eGovFrame Introduction. https://www.egovframe.go.kr/eng/sub.do?menuNo=8
- Kalogirou Victoria, Antonis Stasis, and Yannis Charalabidis. DIGIT D.2, ICEGOV2020. Adapting National Interoperability Frameworks Beyond EIF 3.0: The case of Greece. https://ec.europa.eu/isa2/sites/isa/files/icegov2020_day2_session5_victoria_kalogirou_final_version.pptx
- Nordic Institute for Interoperability Solutions. X-ROAD®. https://x-road.global/
- NIA. GDX Report (2022-1). Digital society development and implications through data sharing and connection - Focusing on the case of X-tee in Estonia. https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=39485&bcIdx=24656&parentSeq=24656
- Christiansen and Gotze (2007), Trends in Governmental Enterprise Architecture: Reviewing National EA Programmes, https://www.researchgate.net/publication/233728993_Trends_in_Governmental_Enterprise_Architecture_Reviewing_National_EA_Programs/citations
- European Commission. Join up – X-Road Data Exchange Layer. https://joinup.ec.europa.eu/collection/ict-security/solution/x-road-data-exchange-layer/about
- e-Estonia. Interoperability services – NIIS. https://e-estonia.com/solutions/interoperability-services/niis/
- NIIS. X-Road Data Exchange Layer. https://digiexpo.e-estonia.com/e-governance/e-government-foundations/x-road-data-exchange-layer/
- PBS News Hour. How Estonia built a digital first government - Interview with Professor Robert Krimmer (Tallinn University of Technology). https://www.youtube.com/watch?v=kHiq5UfxePA

II.7 Приложение: Содержание Каталога технических стандартов (TSC, версия 6.2).

Введение	Изменения по сравнению с предыдущей версией
	Рассматриваемые вопросы
Соединение	Таблица 1: Характеристики межсетевого взаимодействия
	Таблица 2: Характеристики веб-служб
Интеграция данных	Таблица 3: Характеристики интеграции данных
	Рисунок 1: Прямая модель XML
	Рисунок 2. Обмен через промежуточное программное обеспечение
Метаданные управления контентом	Таблица 4. Характеристики метаданных управления контентом
	Таблица 5: Характеристики идентификаторов
Доступ к электронным услугам	Таблица 6: Характеристики компьютерных рабочих станций
	Таблица 7: Характеристики других каналов
	Таблица 8: Характеристики мобильных телефонов
	Таблица 9. Характеристики систем конференц-связи через IP
	Таблица 10: Характеристики систем VoIP (передача голоса по IP)
	Таблица 11a: Характеристики смарт-карт – определение данных
	Таблица 11b: Характеристики смарт-карт – приложения, включая мультиприложения
	Таблица 11c: Характеристики смарт-карт – электрические
	Таблица 11d: Характеристики смарт-карт — протоколы связи
	Таблица 11e: Характеристики смарт-карт – физические
	Таблица 11f: Характеристики смарт-карт – безопасность
	Таблица 11g: Характеристики смарт-карт – терминальная инфраструктура
	Таблица 12: Характеристики обмена биометрическими данными
	Таблица 13. Характеристики смарт проездных документов
	Таблица 14: Характеристики по обеспечению доступности и удобства использования
Характеристики для сфер деятельности	Таблица 15: Характеристики для сфер деятельности – разное
	Таблица 16: Характеристики для сфер деятельности – электронное обучение
	Таблица 17: Характеристики для сфер деятельности – электронное здравоохранение и социальная помощь
	Таблица 18: Характеристики для сфер деятельности – финансы
	Таблица 19: Характеристики для сфер деятельности – торговля, закупки и логистика
	Таблица 20. Характеристики для сфер деятельности – рабочие процессы и веб-сервисы
Appendices	Приложение A: Сокращения и аббревиатуры, используемые в e-GIF
	Приложение B: Глоссарий терминов метаданных

III. Методика описания архитектуры, разработанная Open Group (TOGAF) и ЗАДАЧИ УПРАВЛЕНИЯ информационных И СМЕЖНЫХ технологий (COBIT)

III.1. Введение

Динамичная цифровая среда усилила потребность в оптимизированной архитектуре данных и беспрепятственном обмене данными между корпоративными системами. Два преобладающих рамочных стандарта, Методика описания архитектуры, разработанная Open Group (англ. The Open Group Architecture Framework) (TOGAF) и Задачи управления информационных и смежных технологий (англ. Control Objectives for Information and Associated Technology) (COBIT), содержат важную информацию. Эти стандарты особенно полезны для государственного сектора, который стремится адаптировать и внедрять передовые цифровые решения. Архитектура предприятия помогает объединить изолированные процессы в целостную среду, которая способствует изменениям и согласуется с интегрирующей бизнес-стратегией. Ключевые факторы успешной ИТ-стратегии включают эффективное управление информацией и цифровую трансформацию. Архитектура предприятия предлагает стратегическую дорожную карту для расширения цифровых возможностей, обеспечивающую быструю адаптацию к бизнес-среде.

И COBIT, и TOGAF являются известными методологиями, подходящими для управления ИТ-инфраструктурой и формирования архитектуры предприятия. Они доказали свою особую эффективность в различных реальных приложениях, помогая организациям в достижении их стратегических целей. В процессе выбора между COBIT и TOGAF для управления ИТ и архитектурой предприятия необходимо четко определить потребности и цели реализующего органа. В этом плане поучительным является пример Южной Кореи. Национальное агентство по вопросам информационного общества (NIA) Южной Кореи использовало COBIT в своих инициативах по аудиту ИТ. С другой стороны, Общегосударственный план архитектуры предприятий в Корее (GEAP) в значительной степени опирается на TOGAF. Эти конкретные примеры применения подчеркивают важность для организаций, особенно государственных органов, выбора методологии, соответствующей их стратегическим целям. В настоящей публикации будут подробно рассмотрены преимущества COBIT и TOGAF, а также проанализировано как практическое применение этих методологий в Южной Корее может дать ценную информацию другим странам.

В контексте хранения и обмена данными TOGAF и COBIT являются ценными стандартами, каждый из которых открывает уникальные перспективы для внедрения цифровых технологий в государственном секторе. В TOGAF большое внимание уделено стандартам данных для обеспечения их совместимости и совместного использования определений. комментируя TOGAF, США и Канада приложили усилия для гармонизации своих баз данных с общей стандартной терминологией. В COBIT, напротив, рассматривается более широкий подход, уделяя особое внимание управлению ИТ на уровне предприятия. Это различие подчеркивает важный урок: выбор стандарта влияет не только на управление данными, но и на то, как установить связи для интеграции данных в различных базах данных. В этом контексте Корея представляет собой интересный пример; в таких документах Кореи как «Стандарт предоставления публичных данных», «Руководство по стандартизации баз данных для государственных учреждений» и «Общая стандартная

терминология» содержится важная информация о создании стандартов данных. Независимо от выбранной методологии, возможность обмениваться данными и легко использовать их остается важным фактором, подчеркивающим необходимость комплексной политики стандартизации данных и управления ими.

III.2. Обзор методологий систем хранения и обмена данными

III.2.1 TOGAF

III.2.1.1 Введение в TOGAF

TOGAF (The Open Group Architecture Framework) — это методология описания архитектуры предприятия, используемая для разработки архитектуры внутри организаций. Она была разработана Архитектурным форумом Open Group, на основе TAFIM Министерства обороны США. TOGAF — это находящийся в свободном доступе стандарт, который можно адаптировать и кастомизировать в соответствии с уникальными требованиями организации. Внедрение эффективной архитектуры предприятия, особенно созданной на основе стандарта TOGAF, дает огромные преимущества, напрямую способствуя улучшению управления, цифровым инновациям и экономическому прогрессу во многих аспектах. Стандарт TOGAF предлагает структурированный подход к оптимизации бизнес-операций и повышению гибкости организации, что обеспечивает конкурентное преимущество. Он способствует созданию единой цифровой среды на предприятии, улучшая функциональную совместимость, упрощая управление системой и сокращая затраты на разработку и обслуживание программного обеспечения. TOGAF значительно снижает сложность бизнеса и ИТ, оптимизируя окупаемость инвестиций в существующую инфраструктуру. Он также повышает стратегическую гибкость, сводя к минимуму риск, связанный с новыми инвестициями, и снижая стоимость их владения. Более того, TOGAF упрощает процессы закупок, ускоряя принятие решений без ущерба для архитектурной согласованности. Это помогает экономически выгодным образом приобретать открытые системы от разных поставщиков. В частности, метод разработки архитектуры (Architecture Development Method, ADM) TOGAF предлагает комплексный, пошаговый подход к проектированию и реализации корпоративной архитектуры.

Все мероприятия постоянно совершенствуют и реализуют архитектуру, позволяя организациям устойчиво и целенаправленно адаптироваться к своим бизнес-целям и возможностям. Этапы ADM:

- ***Предварительный этап*** описывает подготовительные и начальные действия, необходимые для создания архитектурных возможностей, включая кастомизацию TOGAF и определение принципов архитектуры.
- ***Фаза A:*** архитектурное видение описывает начальный этап цикла разработки архитектуры. Он включает в себя информацию об определении объема инициативы по разработке архитектуры, определении заинтересованных сторон, создании архитектурного видения и получении одобрения на продолжение разработки архитектуры.
- ***Фаза B:*** бизнес-архитектура описывает разработку бизнес-архитектуры в поддержку согласованного архитектурного видения.

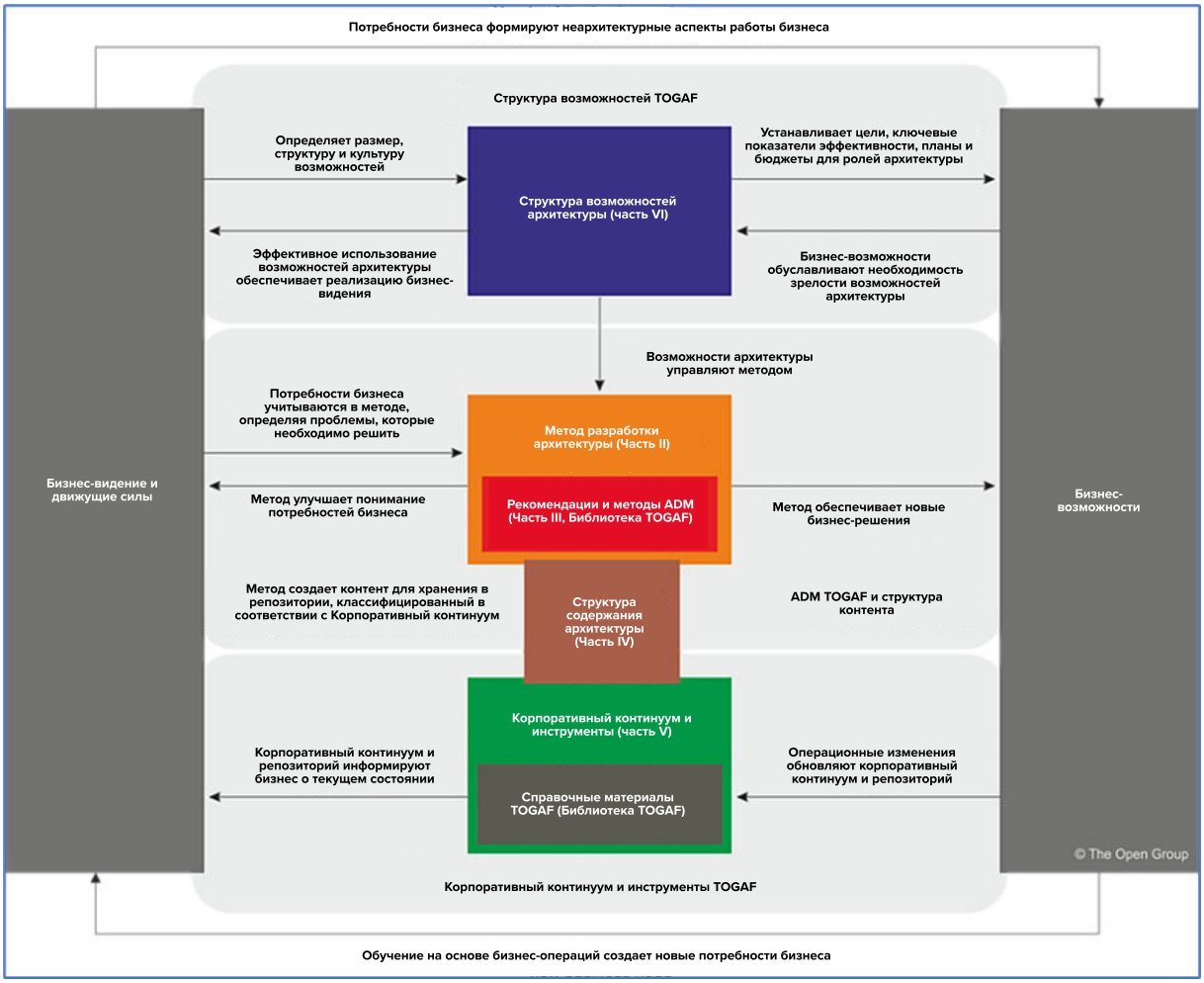
- ***Фаза C:*** архитектура информационных систем описывает разработку архитектуры информационных систем для поддержки согласованного архитектурного видения.
- ***Фаза D:*** техническая архитектура описывает разработку технической архитектуры для поддержки согласованного архитектурного видения.
- ***Фаза E:*** на этапе «Возможности и решения» осуществляется первоначальное планирование внедрения и определение способов обеспечения архитектуры, определенной на предыдущих этапах.
- ***Фаза F:*** планирование миграции посвящена переходу от базовой архитектуры к целевой путем завершения детального плана внедрения и миграции.
- ***Фаза G:*** управление внедрением обеспечивает архитектурный надзор за внедрением.
- ***Фаза H:*** управление изменениями архитектуры устанавливает процедуры управления изменениями в новой архитектуре.
- ***Управление требованиями*** к архитектуре исследует процесс управления требованиями к архитектуре в рамках ADM.

Вставка 7: Стандартный документ TOGAF

- ***Метод разработки архитектуры (Architecture Development Method, ADM):*** ADM предлагает организациям структурированный, пошаговый процесс разработки архитектуры предприятия, охватывающий этапы ее проектирования, планирования, внедрения и управления. В частности, для государственных органов ADM может сыграть важную роль в цифровизации государственных услуг и повышении интероперабельности между ведомствами.
- ***Руководства и методы ADM:*** эта часть стандарта TOGAF содержит полный набор руководств и методов для применения подхода TOGAF и ADM. Эти руководства могут помочь организациям адаптироваться к изменениям и повысить эффективность управления сложными архитектурными проектами.
- ***Фреймворк содержания архитектуры (Architecture Content Framework).*** эта часть TOGAF представляет собой структурированную метамодель для создания архитектурных артефактов. Он помогает создавать четкую, последовательную архитектурную документацию, понятную и удобную для использования всеми заинтересованными сторонами в организации, включая нетехнических лиц, принимающих решения.
- ***Совокупность на уровне предприятия и инструменты (Enterprise Continuum & Tools):*** В этом разделе представлена информация о соответствующей таксономии и инструментах для категоризации и хранения результатов работы с архитектурой. Он помогает организациям эффективно управлять архитектурными ресурсами и повторно использовать их в различных проектах.
- ***Фреймворк возможностей архитектуры (Architecture Capability Framework).*** этот фреймворк определяет организацию, процессы, навыки, роли и обязанности, необходимые для создания и управления функцией архитектуры. Он может помочь в формировании эффективной команды архитекторов и управлении возможностями архитектуры в организации.

Источник: https://www.opengroup.org/togaf-licensed-downloads.

Рис. 10: Структура TOGAF



Источник https://pubs.opengroup.org/architecture/togaf9-doc/arch/.

III.2.1.2 Ключевые компоненты TOGAF

В TOGAF мы можем найти решения о том, как поддерживать и обеспечивать интероперабельность при обмене и хранении данных, на этапе C: Архитектура информационных систем — Архитектура данных. Здесь описывается разработка архитектур данных и приложений. Цель состоит в том, чтобы разработать целевую архитектуру информационных систем, которая описывает как архитектура информационных систем предприятия будет способствовать реализации бизнес-архитектуры и архитектурного видения таким образом, чтобы учитывать требования Заявления об архитектурных работах и проблемы заинтересованных сторон, а также определить возможную дорожную карту архитектуры.

В основные входные данные для архитектуры данных входят:

- Принципы данных.
- Репозиторий архитектуры: повторно используемые строительные блоки (особенно определения текущих данных), общедоступные эталонные модели, эталонные модели для конкретной организации, стандарты организации.
- Предварительный документ с определением архитектуры: базовая архитектура данных, целевая архитектура данных.

- Предварительная спецификация требований к архитектуре: результаты анализа пробелов (из бизнес-архитектуры).

Важно подчеркнуть основополагающую роль общедоступных эталонных моделей, эталонных моделей для конкретной организации и стандартов организации в построении архитектуры данных. Крайне важно опираться на модели данных для конкретных секторов, например, для сельского хозяйства, управления чрезвычайными ситуациями и других областей. Такие модели повышают общенациональную совместимость в соответствующих секторах. Более того, когда организации внедряют согласованные модели данных, они обеспечивают единообразие хранения и обмена данными, что способствует улучшению понимания и сотрудничества между системами. Эти стандартные модели, наряду с эталонными моделями и организационными стандартами, в совокупности создают надежную основу, обеспечивая беспрепятственный обмен и интерпретацию данных в различных системах. Одним из основных результатов архитектуры данных являются требования к совместимости данных.

III.2.1.3 Процесс внедрения TOGAF

Для реализации архитектуры данных необходимо выбрать применяемые стандарты для каждого набора данных и подготовить такие документы, как модель бизнес-данных, логическая модель данных, модель процесса управления данными, матрица объекта данных/бизнес-функции, требования к совместимости данных (например, схема XML)., политика безопасности).

TOGAF также содержит рекомендации по требованиям к интероперабельности. Интероперабельность определено в TOGAF как «способность обмениваться информацией и услугами». Определение степени совместного использования информации и услуг является очень полезным архитектурным требованием, особенно в сложной организации и/или расширенном предприятии. В Архитектуре данных описывается использование модели обмена корпоративными данными и/или информацией. В TOGAF реализация интероперабельности требует создания, управления, принятия и соблюдения реалистичных SMART стандартов (конкретных, измеримых, действенных, реалистичных и ограниченных по времени). В примере Министерства национальной обороны Канады и НАТО может быть четыре степени интероперабельности:

- ***Степень 1:*** обмен неструктурированными данными включает обмен данными, которые могут быть интерпретированы человеком, такими как свободный текст, содержащийся в оперативных оценках, анализе и документах.
- ***Степень 2:*** обмен структурированными данными включает обмен данными, которые могут быть интерпретированы человеком, предназначенными для ручной и/или автоматической обработки, но требует ручной компиляции, получения и/или отправки сообщений.
- ***Степень 3:*** беспрепятственное совместное использование данных предполагает автоматический обмен данными между системами на основе общей модели обмена данными.

- ***Степень 4:*** беспрепятственный обмен информацией является расширением степени 3 для универсальной интерпретации информации посредством обработки данных на основе взаимодействующих приложений.

Рис. 11: Матрица интероперабельности в TOGAF

Фаза B: Требования к интероперабельности информации между заинтересованными сторонами (*на основе степеней интероперабельности информации*)							
Заинтересованные стороны	A	B	C	D	T	F	G
A		2	3	2	3	3	3
B	2		3	2	3	2	2
C	3	3		2	2	2	3
D	2	2	2		3	3	3
E	4	4	2	3		3	3
F	4	4	2	3	3		2
G	2	2	3	3	3	3	

Источник: The Open Group

Матрица интероперабельности бизнес-информации в TOGAF полезна для того, чтобы оценить, исходя из четырех степеней на каком уровне внутренние заинтересованные стороны должны обмениваться друг с другом данными.

Использование зрелых архитектурных возможностей на крупном предприятии позволяет получить широкий спектр архитектурных результатов. Чтобы эффективно управлять этими результатами и использовать их, необходима формальная таксономия для различных типов архитектурных активов. Это должно сопровождаться специальными процессами и инструментами, предназначенными для хранения архитектурного контента. В этом контексте репозиторий архитектуры в Enterprise Continuum and Tools предлагает структурированную основу для информационной базы стандартов. Кроме того, Справочная библиотека содержит рекомендации, шаблоны, алгоритмы и другие формы справочных материалов. Эти ресурсы можно использовать для ускорения создания новых архитектур предприятия. Типами стандартов являются юридические и нормативные обязательства, отраслевые стандарты и организационные стандарты, которые также указаны в архитектуре данных. Классификация стандартов в Информационной базе стандартов следующая:

Бизнес-стандарты:

1. Стандартные общие бизнес-функции
2. Стандартные определения ролей и актеров
3. Стандарты безопасности и управления бизнес-деятельностью

Стандарты данных:

1. Стандартное кодирование и значения данных
2. Стандартные структуры и форматы данных
3. Стандарты происхождения и владения данными
4. Ограничения репликации и доступ к данным

Стандарты приложений:

1. Стандартные/совместные приложения, поддерживающие определенные бизнес-функции
2. Стандарты связи и взаимодействия приложений
3. Стандарты доступа, представления и стиля

Технические стандарты:

1. Стандартные аппаратные продукты
2. Стандартные программные продукты
3. Стандарты разработки программного обеспечения

В контексте стандартов хранения и обмена данными важно подчеркнуть, как TOGAF отличает стандарты данных от стандартов приложений. В последнее время многие организации осознали необходимость стандартов данных не только в рамках стандартов приложений. Это связано с тем, что стандарты данных ориентированы на обмен данными специально для анализа данных на основе искусственного интеллекта, а не просто для услуг, управляемых приложениями.

III.2.2 COBIT

III.2.2.1 Введение в COBIT

COBIT (Задачи управления для информационных и смежных технологий, англ. Control Objectives for Information Related Technology Framework) — это рамочный стандарт, разработанный ISACA (Международная профессиональная ассоциация ИТ). ISACA является глобальной профессиональной членской ассоциацией, предоставляющей услуги лицам, работающим или интересующимся сферами ИТ-аудита, ИТ-рисков и управления ИТ. COBIT 2019 является новейшей редакцией всемирно признанной системы управления корпоративной информацией и технологиями (EGIT) ISACA. Документ COBIT 2019 разработан с целью предоставить заинтересованным сторонам комплексное руководство по достижениям и основным принципам системы COBIT. В нем представлены новые концепции и терминология, а также дается разъяснение базовой модели COBIT и ее 40 задач управления. Кроме того, имеется несколько специализированных направлений и руководящих документов, дополняющих основной документ:

- *Программа аудита COBIT для DevOps:* эта программа направлена на применение принципов COBIT к DevOps, помогая предприятиям оценивать и улучшать свою систему управления DevOps.
- *Задачи управления ИТ для Сарбейнса-Оксли, 4-е издание:* руководство, содержащее инструкции по оценке эффективности внутреннего контроля за финансовой отчетностью в соответствии с Законом Сарбейнса-Оксли.
- *COBIT 2019 для малых и средних предприятий:* специальное руководство для малых и средних предприятий, намеренных применять модель COBIT 2019 в своих организациях.
- *Приоритетные области COBIT:* эти публикации посвящены конкретным темам и содержат рекомендации по применению принципов COBIT в таких областях, как DevOps, информационные и технологические риски и информационная безопасность.

- *Руководство по проектированию COBIT 2019:* руководство по практическому использованию COBIT, содержащее советы пользователям по адаптации системы управления к уникальному контексту их предприятия.
- *Руководство по внедрению COBIT 2019:* обновленное руководство, использующее подход, аналогичный предыдущему Руководству по внедрению COBIT 5, но включающее новые концепции COBIT 2019.
- *Внедрение структуры кибербезопасности НИСТ с применением COBIT 2019:* это руководство иллюстрирует применение COBIT 2019 для реализации стандарта кибербезопасности НИСТ, обеспечивая способ улучшения целей в области кибербезопасности.

COBIT призван содействовать гибкому и индивидуальному проектированию и внедрению системы управления ИТ на предприятии (EGIT). COBIT подчеркивает важность корпоративного управления информацией и технологиями (EGIT). EGIT сложно и многогранно. Универсального подхода к разработке, внедрению и поддержанию эффективной системы EGIT в организации не существует. Требуется индивидуальный подход, соответствующий конкретному контексту и потребностям организации. Члены совета директоров и высшее руководство должны нести большую ответственность за ИТ, тем самым способствуя развитию культуры, направленной на максимизацию ценности ИТ. Фокус EGIT направлен на получение ценности от цифровой трансформации и снижение связанных с ней бизнес-рисков. Три основных конечных результата успешного внедрения EGIT включают реализацию выгод, оптимизацию рисков и оптимизацию ресурсов.

- ***Реализация выгод:*** основное внимание уделяется созданию ценности для предприятия посредством ИТ и поддержанию/увеличению ценности существующих инвестиций в ИТ. Ценность ИТ должна согласовываться с ценностями бизнеса и измеряться таким образом, чтобы демонстрировать ее вклад в процесс создания предприятием ценности.
- ***Оптимизация рисков:*** сюда входит устранение бизнес-рисков, связанных с использованием, эксплуатацией и внедрением ИТ на предприятии. Управление рисками направлено на сохранение ценности, при этом управление рисками, связанными с ИТ, интегрировано в подход к управлению рисками предприятия.
- ***Оптимизация ресурсов:*** это обеспечивает предоставление необходимых возможностей и ресурсов для выполнения стратегического плана, включая обновление или замену устаревших систем, обучение ИТ-персонала и использование данных и информации для получения оптимальной ценности.

III.2.2.3 Ключевые компоненты COBIT

Принципы системы и структуры управления COBIT представляют собой основу эффективного управления информационными технологиями в предприятии. Эти принципы служат руководством при разработке, внедрении и управлении системами и структурами управления, с тем чтобы они соответствовали уникальным потребностям предприятия и оставались гибкими в адаптации к изменениям. В соответствии с принципами системы управления, предприятия должны разрабатывать индивидуально спроектированные системы, способные балансировать выгоды, риски и ресурсы,

создавая при этом ценность от информационных технологий. Такие системы должны быть динамичными, адаптивными, разделять руководство и управление, и обеспечивать всесторонний охват всех аспектов деятельности предприятия, связанных с информационными технологиями. С другой стороны, принципы структуры управления предусматривают, что структура должна базироваться на концептуальной модели для обеспечения согласованности и возможностей автоматизации. Структура должна оставаться открытой и гибкой, позволяя внедрять новый контент и решать возникающие проблемы, не нарушая целостность. Важно отметить, что она должна соответствовать соответствующим стандартам, основам и правилам, чтобы гарантировать их соблюдение и использовать передовую практику.

Задачи руководства и управления являются неотъемлемой частью COBIT, обеспечивая соответствие информации и технологий целям предприятия и способствуя их достижению. Эти задачи, всегда связанные с определенным процессом и рядом взаимосвязанных компонентов, делятся на две категории: задачи руководства и задачи управления, каждая из категорий относится к компетенции различных уровней управленческого состава внутри организации. Задачи руководства обычно находятся под контролем совета директоров и исполнительного руководства. Эти цели, сгруппированные в категорию «Оценка, управление и мониторинг» (EDM), включают в себя оценку стратегических вариантов, предоставление рекомендаций высшему руководству по выбранным стратегиям, а также мониторинг реализации и достижения стратегии. Задачи управления, которыми руководствуется высшее и среднее руководство, разделены на четыре области: Координация, планирование и организация (APO); Разработка, приобретение и внедрение (BAI); Предоставление, обслуживание и поддержка (DSS); и Мониторинг, оценка и анализ (MEA). Эти области охватывают стратегическую координацию ИТ, приобретение и интеграцию ИТ-решений, предоставление ИТ-услуг, включая безопасность, а также мониторинг производительности в соответствии с внутренними и внешними стандартами. Вместе они обеспечивают эффективное и результативное управление ИТ-инфраструктурой предприятия, способствуя постоянному совершенствованию и стратегической координации. Благодаря этим задачам руководства и управления COBIT обеспечивает комплексный подход к управлению ИТ предприятия, включая стратегическую координацию, эффективное предоставление ИТ-услуг, а также постоянную оценку и повышение производительности ИТ и их соответствия целям предприятия.

III.2.2.4 Процесс внедрения COBIT

Подход к внедрению COBIT состоит из семи этапов:

- Что нами движет?
- Где мы находимся?
- Где мы хотим оказаться?
- Что нужно сделать?
- Как мы туда попадем?
- Удалось ли выполнить задуманное?
- Как сохранить импульс?

Подход к внедрению COBIT не затрагивает непосредственно вопросы хранения данных и стандартов данных, направленных на обеспечение интероперабельности. Интересен тот факт, что в COBIT термин «интероперабельность» напрямую не используется; вместо этого основное внимание уделяется «взаимосвязям». Тем не менее, один из трех принципов структуры управления гласит: «Структура управления должна соответствовать соответствующим основным стандартам, основам и положениям». COBIT содержит список стандартов, на которые сделаны ссылки. Он соответствует нескольким связанным стандартам и структурам, включая модель зрелости управления данными CMMI. Также в некоторые задачи включено управление данными для эффективного обмена данными как внутри предприятия, так и за его пределами.

- ***APO02 (Управляемая стратегия):*** требуется стратегия цифровой трансформации организации и достижение желаемой ценности посредством дорожной карты по реализации постепенных изменений. В дорожной карте рассматриваются изменения во всех аспектах организации: от каналов и процессов до данных, культуры, навыков, операционной модели и стимулов.
- ***APO14 (Управляемые данные):*** необходимость обеспечения эффективного использования критически важных данных для достижения целей и задач предприятия.
- ***EG11 (Соблюдение внутренней политики):*** количество инцидентов, связанных с несоблюдением политики. Доля заинтересованных сторон, понимающих политику. Доля политик, поддерживаемых эффективными стандартами.
- ***APO03 (Управляемая архитектура предприятия):*** представляет различные строительные блоки, из которых состоит предприятие, их взаимосвязи, а также принципы, определяющие их проектирование и эволюцию с течением времени, чтобы обеспечить стандартное, гибкое и эффективное достижение операционных и стратегических целей.

В EG11 особое внимание уделяется установлению политики внутренних стандартов данных на предприятии. Если стандарт данных официально формализован и применяется внутри организации, это указывает на то, что политика стандартизации данных эффективно реализуется на уровне предприятия. APO03 представляет цели по достижению взаимосвязей внутри данных учреждения.

III.2.3 Внедрение структуры общеорганизационной архитектуры в Южной Корее

Роль информационных технологий становится все более критической для оперативного реагирования организаций реагировать на разнообразные изменения в окружающей среде, влияющие на их деятельность по созданию стоимости. Сложность бизнес-процессов возрастает, и теперь разделение функций бизнеса и ИТ больше не актуально. Когда организации хотят внести изменения в свои системы, чтобы адаптироваться к переменам в окружающей среде, системы часто настолько сложны, что становится сложно определить где и как внести изменения. Им требуется нечто, что позволит легко визуализировать всю ее структуру, подобно схеме здания.

В связи с этим в Южной Корее была внедрена система управления архитектурой (англ. Government-wide Enterprise Architecture, GEAP) с целью организации сложных систем в

простую и понятную форму. Эта система облегчает преобразование сложных систем организаций в необходимый вид. GEAP интегрирует компоненты всей организации, такие как деятельность, приложения, данные, технологии и безопасность, в соответствии с определенными стандартами и процедурами, а затем структурирует их взаимосвязи для эффективной организации информационных систем.

Система управления архитектурой предприятия в Южной Корея была институционализирована через Министерство внутренних дел и безопасности (MOIS)[20]. В соответствии с законом управление архитектурой определяется как «система, которая всесторонне анализирует организационные компоненты, такие как деятельность, приложения, данные, технологии и безопасность, в соответствии с определенными стандартами и процедурами, и затем структурирует их взаимосвязи».

При разработке GEAP Южная Корея использовала такие методологии как ZEAF, FEAF, TEAF, DODAF и TOGAF. Характеристики, преимущества и недостатки других EA и GEAP приведены в таблице ниже.

III.2.3.1 Ключевые компоненты структуры архитектуры предприятия

Для успешного создания архитектуры предприятия (EA) ключевым является разработка надежной структуры архитектуры предприятия (EAF). Несмотря на наличие множества передовых методологий и предложений со стороны правительства в качестве рекомендаций, предприятия могут использовать их в качестве ресурсов для ориентации. Важно, однако, адаптировать структуру в соответствии с уникальными характеристиками предприятия, избегая ее слепого копирования. Обычно EAF формируется на этапе планирования проекта EA. Среди различных компонентов EAF матрица архитектуры четко определяется на этапе структурирования информации в рамках EAF. Таким образом, процесс определения EAF можно рассматривать как процесс достижения консенсуса, обеспечивающий соответствие конкретным требованиям предприятия по изменениям.

Таблица 9: Ключевые компоненты структуры архитектуры предприятия

Категория	Компонент	Описание
Направление/ Руководство	ИТ-политика	Обеспечивает последовательные цели и направления, независимые от систем, архитектуры, инструментов и продуктов, для внедрения и применения ИТ в соответствии с фундаментальной политикой организации.
	Стратегия архитектуры предприятия	Отражает соответствие существующих и новых ИТ-стратегий предприятия видению и целям всей организации. Стратегия включает в себя архитектурное видение и цель.
	Принципы архитектуры	Предлагает объективные критерии для инвестиций и принятия решений, направленных на достижения целей архитектуры предприятия.
	Требования	Относится к общеорганизационным требованиям для реализации стратегии архитектуры предприятия. Требования должны быть сформулированы с учетом всей организации.

[20] Закон об электронном правительстве, статьи 45–47, о внедрении и использовании архитектуры информационных технологий.

Категория	Компонент	Описание
Деятельность по архитектуре предприятия	Модель архитектуры	Определяет модель архитектуры, классифицирующую все ресурсы организации по перспективам и точкам зрения. Модель представлена в виде матрицы, охватывающей все ресурсы предприятия.
	Жизненный цикл	Включает в себя ряд процессов планирования, разработки, применения, обслуживания, контроля и надзора за архитектурой предприятия, каждый из которых имеет конкретную направленность и виды работ.
	Инструменты поддержки	Инструменты для систематической и эффективной поддержки деятельности жизненного цикла. Включают эталонные модели, процедуры, связанные с инвестициями, модели зрелости и системы управления EA.
Практические результаты	Результаты архитектуры	Конечные продукты, разрабатываемые в соответствии с работой по EA. Они определяются с учетом цели и использования EA и могут использоваться с разных точек зрения. Некоторые обязательные результаты определены в Общеправительственном документе по метамодели результатов EA.

Источник https://dataonair.or.kr/db-tech-reference/d-guide/da-guide/?mod=document&uid=247.

III.2.3.2 Процесс реализации EA

Управление архитектурой предприятия (EA) представляет собой важный процесс, включающий ряд шагов, направленных на систематическую организацию и использование EA. Эти мероприятия способствуют обеспечению согласованности и последовательности в общей системе управления информацией. Процесс управления EA не только классифицирует и определяет детали задач, необходимых для эффективного управления EA, но также устанавливает стандартизированные процедуры, форматы документации и правила, соблюдение которых является обязательным.

После того, как EA создана, она применяется и контролируется. Затем EA оценивается на основе изменений в бизнес- или технологической среде, а также ее текущего использования. Определяются необходимые модификации, которые затем интегрируются в информацию по EA, применяемую во всем предприятии.

Для определения процесса управления EA крайне важно централизовать всю работу по EA. В случае, если к существующему ИТ-процессу добавляется лишь процесс изменений и управления EA, есть вероятность того, что этот процесс не будет правильно проведен. Неправильное выполнение процессов, связанных с EA, может привести к утрате актуальности информации EA и возникновению проблем с сохранением целостности этой информации.

Таким образом, важно определить последовательность ИТ-процессов: создание, использование/контроль, оценку, изменение, с точки зрения EA. Проектирование, основанное на информации по EA, обеспечивает целостность такой информации. Распознавание изменений в информации EA в процессах разработки и эксплуатации обеспечивает актуальность информации EA.

Таблица 10: Ключевые компоненты процесса управления EA

Компонент EA	**Цель**	**Мероприятия**
Планирование	Разработать стратегию управления EA и планы эффективного применения и использования EA	Разработка планов достижения EA, которые включают в себя управление EA, а также ее эффективное применение и использование
Управление изменениями	Обеспечить качество и актуальность информации EA для конкретных секторов	Рассмотрение, утверждение и внесение изменений в информацию EA
Контроль за соблюдением	Повысить уровень соответствия EA в различных секторах управления информацией и соответствующих отделах	Проверка и поддержание ссылок на информацию EA и ее соблюдение
Поддержка использования	Повысить степень использования EA	Продвижение, обучение и распространение информации и передового опыта по EA в целях ее эффективного использования
Система управления	Повысить эффективность управления и использования EA	Построение и использование системы управления информацией для EA
Оценка	Выявить возможности для улучшений путем периодической оценки состояния управления и использования EA	Определение модели оценки EA и проведение регулярных оценок для выявления областей, требующих улучшений

Таблица 11: Особенности, преимущества и недостатки различных платформ

	ZEAF	FEAF	TEAF	DoDAF	TOGAF	EA (GEAP)
Функции	• Введено понятие архитектуры в конце 1980-х для понимания хозяйственной деятельности с инженерной точки зрения. • Предлагает концепцию моделирования с точки зрения 5W1H.	• Последняя версия, выпущенная в 2003 году, содержит основные руководящие принципы федерального правительства США. • На основе эталонной модели EAF.	• EAF Казначейства США (наряду с FEAF, DoDAF является репрезентативным EAF).	• Обеспечение совместимости систем вооружения для эффективной оперативной работы.	• Частный альянс по стандартам, Open Group.	• Призван служить стандартом и руководством по внедрению архитектуры предприятия в правительственных и государственных учреждениях.
Преимущества	• Содержит детальную концепцию моделирования в соответствии с 5W1H. • Определяет области хозяйственной деятельности с точки зрения планировщика, владельца, проектировщика, строителя и субподрядчика.	• Не просто моделирование: методика включает в себя конкретные планы реализации. • Использует различные эталонные модели, такие как BRM, DRM, SCRM, TRM, PRM.	• Особое внимание уделяется функциональным перспективам, которые выражают «Как-Где-Когда», информационным перспективам «Что-Сколько-Как часто», организационным перспективам «Кто-Почему» и инфраструктурным перспективам.	• Подробно определяет шаблоны для выходных данных, обеспечивая единообразное и проверенное моделирование. • Содержит подробные определения и форматы для операционных моделей.	• Предлагает конкретные процессы разработки архитектуры — четко определенные взаимосвязи между различными эталонными моделями.	• Включает в себя практически все элементы, связанные с архитектурой предприятия, что делает ее удобной в качестве базовой методики

	ZEAF	FEAF	TEAF	DoDAF	TOGAF	EA (GEAP)
Недостатки	• Определяет даже области с низкой загрузкой с точки зрения информатизации. • Чрезмерно сосредоточен на моделировании, недостаточно определены реальные работы по архитектуре и ее основа.	• Понимание и развитие модели архитектуры четко определены, но отсутствует эволюционный взгляд на организацию и связанные правила.	• Методика сосредоточена на результатах архитектуры предприятия и не хватает доступности для использования. • Отсутствует перспектива в отношении непрерывной корпоративной деятельности.	• В общей корпоративной среде существует вероятность чрезмерных инвестиций, поскольку требуется чрезмерная производительность и точность.	• Введение понятия континуума, основанного на метамодели, затрудняет отражение уникальности организации в этой структуре.	• Представляет только стандартную структуру, рекомендуя конкретное содержание, которое должно быть написано учреждением.

Source https://dataonair.or.kr/db-tech-reference/d-guide/da-guide/?mod=document&uid=247

III.3 Сравнение TOGAF, COBIT, GEAP

Несмотря на частичное совпадение в руководстве и управлении ИТ-ресурсами между TOGAF и COBIT, эти два подхода были разработаны для разных основных целей. COBIT подробно описывает конкретные процессы, но при рассмотрении деталей архитектуры он может оказаться менее конкретным по сравнению с TOGAF. Это не означает, что COBIT в чем-то отстает, а, скорее, подчеркивает содержащийся в нем упор на системы и приложения. TOGAF, напротив, не ограничивается отдельной областью, а охватывает архитектуру приложений, данных, бизнеса и технологий, обеспечивая комплексный взгляд. Одним из достоинств COBIT является его модель оценки возможностей процесса, которая упрощает оценку уровней зрелости ИТ-процессов и предоставляет четкую дорожную карту для их улучшения и развития на уровне предприятия.

Процесс создания архитектуры государственного предприятия (GEAP) Южной Кореи задает направление и обеспечивает руководство для ИТ-политики, стратегии архитектуры предприятия, принципов архитектуры и требований. Одним из примечательных аспектов GEAP является Закон об информационных системах, принятый в 2005 году. Согласно этому закону, все проекты, связанные с ИТ, подлежат регистрации на общеправительственном сайте GEAP. Это обеспечивает прозрачность, поскольку все государственные учреждения Кореи могут получить доступ к любой системе, созданной в государственном секторе Кореи, и осуществлять поиск по ней. Такой подход не только предотвращает избыточные проекты, что приводит к экономии бюджета, но и повышает эффективность по всем направлениям. Кроме того, несмотря на то, что GEAP охватывает практически все вопросы, связанные с архитектурой предприятия, он также обладает гибкостью, позволяющей учреждениям разрабатывать детальное содержание, адаптированное к их уникальным потребностям.

Основные особенности и преимущества каждого стандарта приведены здесь и в Таблице 5 ниже:

- ***TOGAF:*** комплексный взгляд на архитектуру, охватывающий приложения, данные, бизнес и технологии, обеспечивает адекватный учет всех направлений. Такой широкий охват дает предприятиям общее представление, необходимое для принятия стратегических решений и соответствия бизнес-целям.
- ***COBIT:*** модель оценки возможностей процесса является его сильной стороной. Организации могут сравнить свои ИТ-процессы с отраслевыми стандартами, понять, где они находятся, и получить понимание, где требуются улучшения. Такой структурированный подход обеспечивает развитие ИТ-процессов в соответствии с бизнес-требованиями, обеспечивая оптимальное использование ИТ-ресурсов.
- ***GEAP:*** обязательная регистрация ИТ-проектов в соответствии с Законом об информационных системах обеспечивает прозрачность и подотчетность. Централизованный репозиторий служит базой знаний, гарантируя избежание повторения ошибок и распространение передового опыта во всех учреждениях. Гибкость методологии GEAP также гарантирует, что учреждения не будут принуждены использовать универсальный подход, а смогут адаптировать руководящие принципы к своему конкретному контексту.

добиться их большей эффективности при обмене данными. В связи с этим правительства США и Канады предприняли усилия по установлению единого стандарта данных для всех государственных органов. В частности, в США действует Национальная модель обмена информацией (NIEM). NIEM включает общий стандарт данных (NIEM Core) и специализированные стандарты данных (NIEM domains), принятые руководящими группами для конкретных областей.

Следовательно, с точки зрения хранения и обмена данными существует острая необходимость в более детальном подходе и методологии практического управления данными. Цель обмена данными и интеграции выходит за рамки простых ИТ-услуг. Это также имеет решающее значение для искусственного интеллекта и анализа данных. Отсутствие стандартизированного хранения и управления данными может повлечь за собой значительные затраты. В этом контексте организационные и общеотраслевые модели и стандарты данных во всех странах становятся обязательными для максимизации потенциала данных.

Таблица 12: Сравнение TOGAF, COBIT, GEAP

Методология	Ключевые компоненты	Сильные стороны	Слабые стороны	Примеры успешного использования
TOGAF	• Фаза A: Архитектурное видение • Фаза B: Бизнес-архитектура • Фаза C: Архитектура информационных систем • Этап D: Техническая архитектура • Фаза E: Возможности и решения • Фаза F: Планирование миграции • Фаза G: Управление реализацией • Фаза H: Управление изменениями архитектуры	• Предложение по процессу разработки конкретной архитектуры • Четко определенные взаимосвязи использования различных эталонных моделей. • С точки зрения совместимости данных последовательно представляет управление стандартами данных на уровне организации. • Представлены различные инструменты и матрицы, которые можно использовать с точки зрения увязки данных, что упрощает их применение на практике.	• Отсутствие методологии управления стандартами и увязки данных, такой как DRM (эталонная модель данных). • Отсутствие важных областей данных и кодов с точки зрения обмена данными. • Хотя TOGAF содержит методологии оценки, он не предлагает конкретные шаблоны для управления стандартами.	• Dairy Farm Group (Гонконг): сделана ссылка на Информационную базу стандартов TOGAF (SIB). • Департамент социального обеспечения (Великобритания): включил в свой подход Информационную базу стандартов (SIB).
COBIT	• Процессы • Организационные структуры и рамки • Принципы, политика и процедуры • Информация • Культура, этика и поведение • Люди, навыки и компетенции • Услуги, инфраструктура и приложения	• Обеспечение индивидуального подхода, соответствующего конкретному контексту и потребностям организации. • Упор на координацию ИТ на предприятии, с постоянной оценкой и повышением производительности и совместимости ИТ.	• Как методология, рассматриваемая с точки зрения ИТ-аудита, ее содержание в первую очередь построено вокруг управления системой на уровне предприятия. • Больше упор на межсистемные связи, а не на стандарты данных. • Вместо того чтобы рассматривать обмен данными и стандарты отдельно, COBIT подходит к ним с точки зрения системной интеграции для достижения институциональных целей.	• Таможня Дубая: Внедрена единая структура и система управления на основе COBIT. • Муниципалитет Саудовской Аравии: принят COBIT в качестве стандарта управления предприятием и услугами.

Методология	Ключевые компоненты	Сильные стороны	Слабые стороны	Примеры успешного использования
GEAP (Южная Корея)	• Руководство (ИТ-политика, стратегия архитектуры предприятия, принципы архитектуры, требования) • Архитектура предприятия (модель архитектуры, инструменты поддержки) • Результаты (Результаты архитектуры)	• Закон об эффективном внедрении и эксплуатации информационных систем от 30 декабря 2005 года. Все системы, базы данных, программное и аппаратное обеспечение, создаваемые в результате каждого ИТ-проекта, подлежат регистрации на общеправительственном сайте GEAP (www.geap.go.kr) • Все государственные учреждения Кореи могут осуществлять поиск по каждой системе, созданной в государственном секторе Кореи. Это позволяет им предотвращать избыточные проекты, что приводит к экономии бюджета и повышению эффективности. • Легко используется в качестве базовой методологии, поскольку включает в себя почти все элементы, связанные с архитектурой предприятия.	• Представляет только стандартную методологию, рекомендуя учреждениям самим разрабатывать подробное содержание. • Был сделан сдвиг в сторону общегосударственной системы управления ИТ-проектами (GEAP), а построение EA (архитектуры предприятия) управляется индивидуально с учетом конкретных потребностей каждого учреждения.	• ресурсов, инфраструктуры и транспорта: Интеграция EA в планирование и бюджетирование при поддержке руководства. • Статистическое управление Кореи: проведена оценка всех ИТ-проектов • Мегаполис Пусан: координация EA со сбалансированной системой показателей • Мегаполис Сеул: Достигнута значительная экономия благодаря тщательному ежегодному анализу проектов EA. • Мегаполис Ульсан: оптимизированное планирование ИТ • KEPCO: Существенная экономия бюджета в 2010-2011 гг. • Корейский институт ядерной медицины: курирование задач от начала до завершения.

III.4. Презентация вариантов использования и передовой практики (примеры Кореи)

Опираясь на такие рамочные стандарты, как TOGAF и COBIT, GEAP в Южной Корее выполняет роль комплексной схемы, систематически организующей основные атрибуты системы, включая задачи обработки, аппаратное и программное обеспечение продукта, данные и прикладные технологии.

В области использования и управления корпоративной архитектурой GEAP в Южной Корее демонстрирует различные примеры успешной интеграции как в государственном, так и в частном секторах. Такая интеграция отражает не только приверженность информационному управлению, но также стремление к оптимизации ресурсов.

- ***Министерство земельных ресурсов, инфраструктуры и транспорта:*** будучи признанным пионером в создании, управлении и использовании EA, министерство активно использует ее в процессах информационного планирования и бюджетирования. Твердая приверженность генерального директора, директора по информационным технологиям и отдела, ответственного за ИТ, свидетельствует о его непоколебимом внимании. Кроме того, министерство разработало систему для интеграции и управления информацией EA от аффилированных и дочерних организаций.

- ***Статистическое управление Кореи:*** институционализация присутствует на каждом этапе информационного планирования на основе EA, выполнения проектов и управления эффективностью. Специально созданный комитет по рассмотрению ИТ-инициатив тщательно анализирует даже обычные задачи и общие бюджеты бухгалтерского учета. Директор по информационным технологиям постоянно следит за информацией EA.

- ***Мегаполис Пусан:*** достижения EA переплетаются со Сбалансированной системой показателей (BSC) учреждения. В соответствии с «Правилами эксплуатации архитектуры информационных технологий» главным ответственным сотрудником был назначен сотрудник по планированию и финансам. У них есть отдельные команды для продвижения и использования EA, а оценка BSC включает показатели производительности EA.

- ***Мегаполис Сеул:*** являясь одним из первых государственных предприятий, внедривших EA, город Сеул успешно внедрил соответствующую систему управления и использования. Благодаря ежегодному обзору проектов на основе EA и управлению информацией были получены ощутимые выгоды. Например, анализ целесообразности бюджета в 2011 году привел к экономии 54,4 млрд. вон по 20 проектам и еще 3,99 млрд. вон за счет интеграции четырех проектов.

- ***Мегаполис Ульсан:*** город использует Национальную EA для предотвращения избыточных инвестиций во время планирования ИТ-проектов и управления ресурсами.

- ***KEPCO:*** их приверженность EA очевидна благодаря специальной организации под непосредственным руководством генерального директора. Группа планирования ИКТ курирует все ИТ-проекты, стандартизацию данных и систематическое управление производительностью EA. Примечательно, что в период с 2010 по 2011 год предварительный анализ ИТ-проектов позволил сэкономить бюджет в размере 600 млн. вон.

- ***Корейский институт ядерной медицины:*** приступил к созданию системы управления ИТ с точки зрения EA. С помощью EAMS они управляют компьютерными задачами, анализом воздействия, разработкой и эксплуатацией.

Эталонная модель в EA представляет собой стандартизацию архитектурных компонентов, определенных для выделения главных признаков. Она служит абстрактной моделью, к которой обращаются учреждения или предприятия при создании своей корпоративной архитектуры. Эталонная модель абстрагирует концептуальную модель системы, обеспечивая ее соответствие различным точкам зрения. Кроме того, она предоставляет компоненты многократного использования, что облегчает его применение на нескольких предприятиях.

Также рекомендуется использовать определенные эталонные модели для отраслей со схожими характеристиками. Каждое предприятие может черпать вдохновение из общей эталонной модели для своего сектора, что способствует разработке уникальной архитектуры.

Существуют различные эталонные модели, в том числе эталонная бизнес-модель (BRM), эталонная модель данных (DRM), эталонная модель услуг (SRM), техническая эталонная модель (TRM) и эталонная модель производительности (PRM).

- ***Эталонная модель производительности (PRM):*** представляет элементы, показатели и методы измерения результатов производительности ИТ.
- ***Эталонная бизнес-модель (BRM):*** служит эталоном бизнес-архитектуры, классифицируя и определяя бизнес или задачи целевого учреждения.
- ***Эталонная модель услуг (SRM):*** действует как стандарт для архитектуры приложений, классифицируя и определяя функциональные возможности услуг приложений.
- ***Эталонная модель данных (DRM):*** устанавливает руководящие принципы для архитектуры данных, анализируя основные элементы данных, которыми обмениваются учреждения, а также их дальнейшее определение и стандартизацию.
- ***Техническая эталонная модель (TRM):*** устанавливает критерий технической архитектуры, классифицируя и идентифицируя информационные технологии.

Давайте рассмотрим эталонную бизнес-модель (BRM), эталонную модель услуг (SRM) и эталонную модель данных (DRM) с точки зрения стандартов хранения и обмена данными. Эталонная бизнес-модель (BRM) — это эталонная модель, определяющая функции, основанные на независимых бизнес-операциях учреждения. По состоянию на 2020 год в Южной Корее она разделена на 17 областей политики, 71 область политики, 523 основные

функции, 1833 вторичные функции и 9558 третичных функций. Единицы операций, определенные в BRM, не обязательно соответствуют задачам, выполняемым конкретным учреждением. Вместо этого они означают, /что независимо от цели и характера задач, которые берет на себя учреждение, эти задачи могут быть описаны с использованием единиц операций, изложенных в BRM. Это обеспечивает общий ориентир для бизнес-анализа, который позволяет учреждениям определять, выполняют ли разные организации схожие задачи, способствуя совместной разработке систем для поддержки аналогичных функций. BRM также может помочь в поиске проектов в других учреждениях, имеющих схожий контент, предлагая точку отсчета.

Эталонная модель услуг (SRM) служит функционально-ориентированной оценочной эталонной моделью, предназначенной для категоризации элементов услуг, которые поддерживают выполнение задач и достижение целей. В первую очередь она предназначена для содействия идентификации приложений в государственном секторе, налаживания связей между задачами и сервисами, поощрения повторного использования и предотвращения избыточной разработки. Это представляет собой стандартную систему классификации услуг, независимую от задач и организационных структур. С помощью этой модели учреждения могут обнаруживать задачи государственного уровня и элементы сервисов приложений. Цель создания SRM — предоставить систему классификации, которая будет способствовать повторному использованию сервисов приложений, а также предложить унифицированную и интегрированную систему классификации для компонентов поддержки задач правительственных учреждений. Он также способствует разработке, накоплению и распространению компонентов между промышленностью и правительством, упрощая идентификацию сложных и разнообразных прикладных услуг государственных ведомств.
По состоянию на 2012 год эталонная модель услуг включает три области услуг: государственные услуги, услуги внутренней государственной поддержки и общие технические услуги.

- ***Государственные услуги*** сосредоточены на поддержке уникальных институциональных задач и реализации проектов. Они соответствует задачам и целям государственных ведомств и включает в себя правила и процедуры выполнения задач. Он состоит из различных сфер, таких как жизнь населения, окружающая среда, национальная инфраструктура, интеллектуальная деятельность, социальное обеспечение, общественное здравоохранение, экономическая деятельность, культурная жизнь, общественная безопасность, а также международные и межкорейские обмены. Этот сектор разделен на 1-й уровень (10 категорий), 2-й уровень (36 категорий) и 3-й уровень (107 категорий).

- ***Услуги внутренней государственной поддержки*** относятся к услугам, которые обычно используют несколько учреждений и предоставляются в интегрированной среде. Они состоят из широко используемых услуг в различных учреждениях, включая аудит, юридические, финансовые, общие административные услуги, управление задачами, связи с общественностью, управление человеческими ресурсами и информатизацию. Этот сектор разделен на 1-й уровень (8 категорий) и 2-й уровень (38 категорий).

- необходимые для реализации как государственных услуг, так и услуг внутренней государственной поддержки. Это компоненты технологических услуг, которые могут широко использоваться в нескольких системах независимо от конкретных задач. Если компоненты в области общих технических услуг усовершенствованы и повторно используются/совместно используются, это может снизить затраты на разработку и управление базовыми функциями при построении информационных систем и обеспечить совместимость между функциями приложений. Этот сектор разделен на 1-й уровень (9 категорий) и 2-й уровень (50 категорий).

Эталонная модель данных (DRM) — это архитектурная структура, предназначенная для облегчения понимания и использования информации в различных организациях. Она определяет стандарты и структуры для поощрения межинституционального обмена данными, стандартизации, повторного использования и управления данными. Давайте рассмотрим каждый из пяти ключевых элементов, составляющих структуру DRM:

- ***Модель данных:*** представляет собой схему всех данных, которые используются и собираются в государственном секторе. Это помогает идентифицировать существующие данные и связи между различными областями данных. Обращаясь к этой модели, отдельные учреждения могут получить ясность относительно того, какие данные в настоящее время создаются, управляются и используются в правительстве.

- ***Классификация данных:*** определяет критерии классификации данных. Данные в общеправительственной модели данных сгруппированы на основе этой классификации. Кроме того, элементы структуры данных сопоставляются с этой системой классификации. Использование этой системы классификации облегчает управление данными и возможности поиска.

- ***Структура данных:*** документируются все элементы данных в пределах области действия, их владельцы, стандартизированные определения элементов и отношения между этими элементами. Он предлагает рекомендации по стандартизации и указатели для создаваемых и используемых элементов данных. В конечном счете, значительные стандартизированные элементы данных регистрируются, чтобы стимулировать совместное использование и повторное использование.

- ***Обмен данными:*** речь идет об установлении стандартов и механизмов обмена данными. Он предоставляет определения целей обмена, структуры сообщений и методов обмена сообщениями. Цель состоит в том, чтобы эффективно управлять историей обмена данными. С помощью определенных здесь пакетов обмена данными к элементам данных можно обращаться и повторно использовать.

- ***Управление данными:*** в этом разделе определяются политики, правила, процессы и организационные структуры, связанные с поддержанием качества данных, стандартизацией и безопасностью. Это важная часть обеспечения того, чтобы данные были надежными, безопасными и соответствовали установленным стандартам.

Опираясь на такие устоявшиеся системы, как TOGAF, COBIT и EA, Южная Корея представила практическую методологию управления общедоступными данными с точки зрения стандартов данных и обмена данными. Согласно Закону об управлении данными в Корее, государственные органы обязаны управлять метаданными базы данных, которые они создают, приобретают и контролируют. Метаданные относятся к представлению структуры, атрибутов, характеристик и истории данных. Это четко изложено в «Руководстве по стандартизации баз данных для государственных учреждений», изданном Министерством внутренних дел и безопасности, которое предписывает 43 стандартных элемента. Благодаря этой системе все метаданные базы данных, от таблиц до столбцов каждого государственного учреждения, управляются в интегрированной системе управления метаданными. Это обеспечивает базовую настройку для эффективного поиска и обмена данными между различными публичными организациями. Чтобы способствовать интеграции и совместному использованию общедоступных данных, Министерство внутренних дел и безопасности разработало единую стандартную терминологию. Эта инициатива направлена на обеспечение согласованности и единообразия модели данных путем стандартизации терминов или названий столбцов, которые часто используются в разных ведомствах. Часто встречающейся проблемой является использование разных терминов, означающих одно и то же, например «номер мобильного телефона» и «сотовый телефон». Введение общей стандартной терминологии является стратегической попыткой обеспечить единое обозначение таких терминов. Расхождения в терминологии и формате неизменно требуют дополнительной обработки, что приводит к дополнительным затратам и затраченному времени.

Однако благодаря внедрению общей стандартной терминологии в базы данных государственных учреждений интеграция данных становится заметно более эффективной. Когда государственные учреждения применяют стандарты в своей деятельности, они должны придерживаться более высоких действующих стандартов. В случае проекта создания или восстановления базы данных необходимо создание стандартов баз данных. На этом этапе база данных должна соответствовать как «Институциональным стандартам» более высокого уровня, так и более широкому государственному стандарту «Общая стандартная терминология».

Кроме того, при формулировании стандартов на организационном уровне использование общей стандартной терминологии является обязательным. Эти принципы также считаются основными критериями проверки при оценке и контроле проектов создания баз данных. Существует 1686 терминов, которые были стандартизированы в соответствии с Общей стандартной терминологией. Общая стандартная терминология Южной Кореи была создана по тем же причинам, что и Ядро национальной модели обмена информацией (NIEM) США. NIEM служит эталонной моделью, обслуживающей широкий спектр направлений, таких как юстиция, морское судоходство, военные операции, досмотр, наземный транспорт, биометрия, ХБРЯ, сельское хозяйство, управление чрезвычайными ситуациями, социальные службы, иммиграция, защита инфраструктуры, разведка и международная торговля.

Такое широкое участие обеспечивает представительство федеральных, государственных, местных, этнических, частных и даже международных организаций. Это помогает в достижении консенсуса относительно терминов, определений, отношений и форматов, не диктуя, как информация должна храниться в отдельных системах. Модель NIEM

включает в себя конкретные элементы, адаптированные к потребностям каждого сообщества. Более того, он содержит основные элементы (NIEM Core), которые получили всеобщее согласие во всех сообществах, использующих NIEM. Некоторыми из этих общепризнанных ключевых элементов являются «человек», «местоположение», «предмет», «организация» и «деятельность». Помимо эталонной модели, NIEM является основополагающим слоем, на котором строится обмен данными. Он не только представляет модель, но также предоставляет четкий набор правил и методологий ее использования. Существует установленный жизненный цикл разработки обмена информацией, который соответствует стандартизированным протоколам, обеспечивая согласованность и возможность повторного использования для всех.

Министерство внутренних дел и безопасности разработало «Стандарт предоставления публичных данных». Это относится к стандарту, который следует применять при предложении наборов и коллекций данных (наборов данных), которые необходимо предоставлять в единообразном формате и с идентичными элементами, учитывая потребности использования частного сектора. Многие учреждения предоставили общедоступные данные в различных форматах. С увеличением объема общедоступных данных и ростом спроса на их использование по состоянию на 2021 год в среднем 64 учреждения предоставляли аналогичные данные в различных формах. Учитывая запросы частного сектора и требования предоставления данных в едином формате и единицах, по состоянию на 2023 год установлено 169 типов Стандартов предоставления публичных данных.

IV. Эталонная архитектура облачных вычислений

IV.1. Введение

В этом документе представлена эталонная архитектура для облачных вычислений. Эталонная облачная архитектура относится к архитектурной модели, которая помогает проектировать и создавать сервисы в среде облачных вычислений. Она служит руководством по разработке стабильных и масштабируемых приложений путем эффективного использования сервисов и технологий, предоставляемых различными поставщиками облачных услуг.

IV.2. Ключевые принципы облачной эталонной архитектуры

Эталонная облачная архитектура должна соответствовать нескольким ключевым принципам, позволяющим пользователям облачных вычислений создавать и использовать стабильные и эффективные приложения в облачной среде. Облака, построенные на этих принципах, помогают пользователям оптимизировать облачные ресурсы, удовлетворить бизнес-требования и повысить безопасность, надежность, эффективность производительности, оптимизацию затрат и эффективность эксплуатации.

- ***Операционное совершенство:*** этот принцип улучшает операционные процессы, повышая доступность системы и снижая затраты. В нем особое внимание уделяется таким элементам, как управление изменениями, мониторинг, реагирование на проблемы и автоматизация.
- ***Надежность:*** принцип надежности помогает при проектировании и эксплуатации систем для того, чтобы противостоять неожиданным сбоям. Он включает в себя такие темы, как устойчивость, эластичность и целостность данных.
- ***Безопасность:*** принципы безопасности относятся к защите данных, систем и сетей. Они охватывают контроль доступа, защиту данных, аутентификацию личности и авторизацию.
- ***Эффективность:*** здесь внимание направлено на рациональное использование ресурсов, охватывая такие темы, как масштабируемость, оптимизация эффективности и управление ресурсами.
- **Оптимизация затрат*:*** принцип оптимизации затрат помогает эффективно использовать облачные ресурсы для снижения затрат. Он включает в себя эффективное управление затратами, изменение размера ресурсов, анализ использования и многое другое.

IV.3. Принципы создания эталонной облачной архитектуры

Многочисленные организации и ассоциации по стандартизации представили эталонные облачные архитектуры, а крупные облачные компании также делятся своими архитектурами облачных вычислений в качестве базы. В этом документе использовались эталонные архитектуры, предоставленные учреждениями или компаниями, в соответствии со следующими принципами:

- Эталонная архитектура основана на облачных архитектурах, разработанных международными организациями по стандартизации, а также на архитектурах, предложенных крупными игроками облачной индустрии.

- Акцент в эталонной архитектуре делается на точку зрения поставщиков облачных услуг, а не на точку зрения пользователей.
- Эталонная архитектура была разработана таким образом, чтобы быть независимой от облачных технологий конкретных компаний.
- Архитектура стремится по возможности включать последние достижения в области технологий облачных вычислений.
- Учитывая существование различных типов облаков, эталонные архитектуры предоставляются на основе репрезентативных типов.
- Поскольку технологии облачных сервисов охватывают широкий спектр функций и включают в себя множество новейших технологий, таких как искусственный интеллект и большие данные, эталонная архитектура в первую очередь ориентирована на представление архитектур, основанных на основных облачных технологиях.

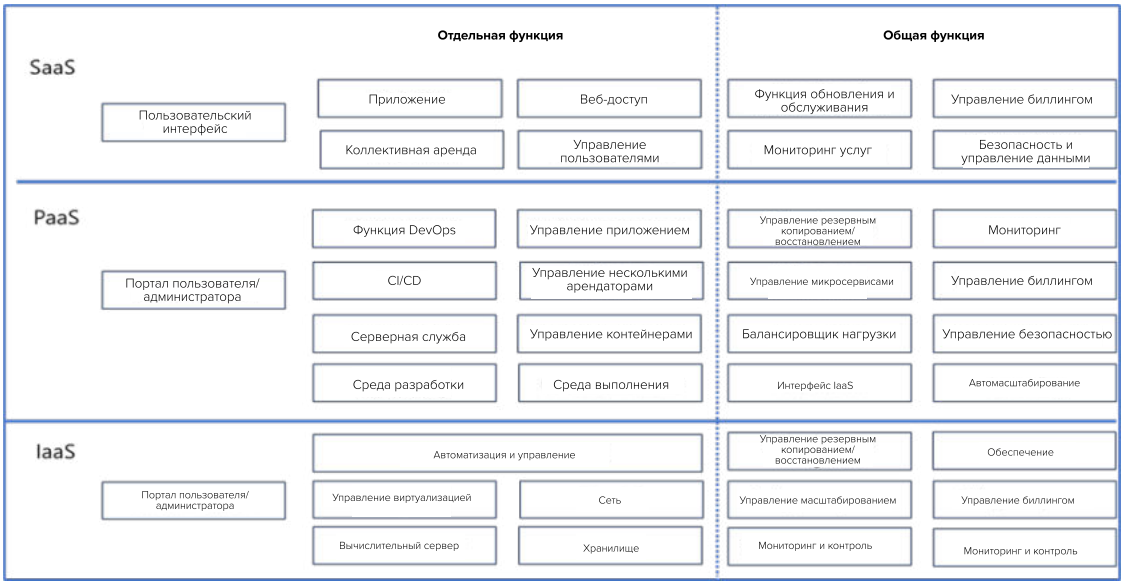
IV.4. Компоненты архитектуры исходя из видов облачных сервисов

Облачные сервисы подразделяются на три основных вида в зависимости от характера предлагаемых ими услуг:

- ***IaaS (Инфраструктура как услуга)*** предполагает, что поставщики облачных услуг предоставляют в аренду оборудование, необходимое для вычислений, в форме услуг.
- ***PaaS (Платформа как услуга)*** включает поставщиков облачных услуг, предлагающих платформы, необходимые для разработки и выполнения приложений.
- ***SaaS (Программное обеспечение как услуга)*** относится к программным приложениям, сдаваемым в аренду в форме услуги поставщиками SaaS.

Эти три типа услуг составляют основополагающие аспекты облачных вычислений, кроме того, существует множество других моделей «как услуга» для удовлетворения разнообразных потребностей.

Рис. 12. Общая архитектура облака.



IV.4.1 IaaS (Инфраструктура как услуга)

IaaS — это одна из моделей услуг облачных вычислений, предоставляющая виртуализированные вычислительные ресурсы для доставки инфраструктуры по требованию. Это инновационное решение снижает затраты на приобретение и управление оборудованием за счет виртуализации существующей локальной инфраструктуры и ее предоставления через Интернет. IaaS предлагает гибкость для масштабирования ресурсов, таких как виртуальные серверы, хранилища и сети, по мере необходимости.

Ключевые компоненты IaaS включают в себя:

- ***Компьютерные серверы:*** относятся к серверным ресурсам, используемым в среде облачных вычислений, использующим виртуализацию для логического разделения и управления аппаратными ресурсами.
- ***Хранилище:*** обеспечивает хранение данных и управление ими через облачное хранилище. Доступны различные типы, такие как блочное хранилище, хранилище файлов и хранилище объектов.
- ***Сеть:*** управляет связью между виртуальными серверами и внешними соединениями через виртуальную сеть. Это включает в себя выделение IP-адресов, настройку брандмауэра, балансировку нагрузки и т.д.
- ***Управление виртуализацией:*** платформы IaaS предоставляют инструменты управления виртуализацией, поддерживающие такие задачи, как создание, управление, мониторинг и масштабирование виртуальных машин.
- ***Автоматизация и управление:*** автоматизирует и управляет такими задачами, как развертывание, предоставление и масштабирование ресурсов, с помощью инструментов автоматизации для повышения операционной эффективности.
- ***Безопасность и соответствие требованиям:*** предоставляет функции и инструменты для обеспечения безопасности и соответствия требованиям, а также обеспечения целостности и конфиденциальности данных.
- ***Управление масштабированием:*** позволяет увеличивать или уменьшать ресурсы в зависимости от спроса, удовлетворяя меняющиеся потребности бизнеса.
- ***Система выставления счетов:*** большинство поставщиков IaaS взимают плату в зависимости от использования ресурсов, которая может динамически меняться в зависимости от фактического использования.
- ***Портал пользователя/администратора:*** портал пользователя и администратора IaaS представляет собой веб-интерфейс, используемый для использования и управления услугами IaaS. Он помогает пользователям управлять и контролировать ресурсы IaaS, а также использовать услуги, предоставляемые поставщиком IaaS.
- ***Обеспечение:*** относится к процессу динамического создания, настройки и развертывания вычислительных ресурсов в облачной среде. Этот процесс имеет решающее значение для эффективного приобретения необходимых вычислительных ресурсов и настройки среды в соответствии с требованиями приложений.

IaaS дает разработчикам и предприятиям возможность разрабатывать, развертывать и эксплуатировать приложения без сложностей управления аппаратной инфраструктурой, предлагая надежную модель облачных вычислений.

IV.4.2 PaaS (платформа как услуга)

PaaS — это модель услуг облачных вычислений, которая предоставляет платформу для разработки, развертывания и управления приложениями. Она абстрагирует инфраструктуру и среду выполнения, позволяя разработчикам сосредоточиться на коде приложения. Это упрощает и ускоряет выполнение задач на протяжении всего жизненного цикла разработки приложений.

Ключевые концепции и компоненты PaaS включают:

- ***Среда разработки:*** PaaS предлагает разработчикам необходимую среду для написания и тестирования кода приложения. Он может включать интегрированные среды разработки (IDE), инструменты разработки, инструменты отладки и т.д.
- ***Исполнительная среда:*** PaaS предоставляет среду исполнения, в которой запускаются приложения. Сюда входят веб-серверы, базы данных, промежуточное программное обеспечение, библиотеки времени выполнения и т.д.
- ***Управление приложениями:*** включает в себя функции управления всем жизненным циклом приложений, обеспечивая простоту эксплуатации и управления.
- ***Функциональность DevOps:*** улучшает сотрудничество между разработкой и эксплуатацией, автоматизирует процессы разработки и развертывания программного обеспечения, способствует общению и сотрудничеству между командами.
- ***Управление контейнерами:*** автоматизирует развертывание, управление, масштабирование и настройку нескольких контейнеров. Он упрощает развертывание и управление крупномасштабными распределенными приложениями и эффективно управляет контейнерными приложениями.
- ***Управление микросервисами:*** в архитектуре микросервисов функции управления включают задачи, связанные с разработкой, развертыванием, мониторингом, масштабированием и управлением независимыми микросервисами. Это обеспечивает стабильность, доступность, производительность и безопасность всей системы.
- ***Предоставление внутренних услуг:*** предлагает различные услуги для разработчиков, позволяющие легко добавлять необходимые функции. Сюда входит управление базами данных, службы обмена сообщениями, службы безопасности и т.д.
- ***Масштабирование и балансировка нагрузки:*** автоматически масштабирует ресурсы и выполняет балансировку нагрузки в зависимости от требований приложения для оптимизации производительности.
- ***Развертывание и управление:*** упрощает развертывание и управление приложениями. Поддерживает контроль версий, автоматическое развертывание, мониторинг, ведение журналов и т.д.

PaaS позволяет разработчикам сосредоточиться на разработке приложений, одновременно снижая нагрузку на управление инфраструктурой, обеспечивая более быструю разработку и развертывание инновационных решений. Эта модель упрощает и ускоряет жизненный цикл разработки программного обеспечения, помогая предприятиям быстрее реагировать на их потребности.

IV.4.3 SaaS (Программное обеспечение как услуга)

SaaS — это модель услуг облачных вычислений, которая предоставляет программное обеспечение через Интернет, доступное через веб-браузеры или мобильные приложения. Пользователи могут получать доступ к программным приложениям и использовать их, не приобретая и не устанавливая. SaaS предлагает удобный способ доступа к различным типам программных приложений как для предприятий, так и для частных лиц.

Ключевые концепции и компоненты SaaS включают в себя:

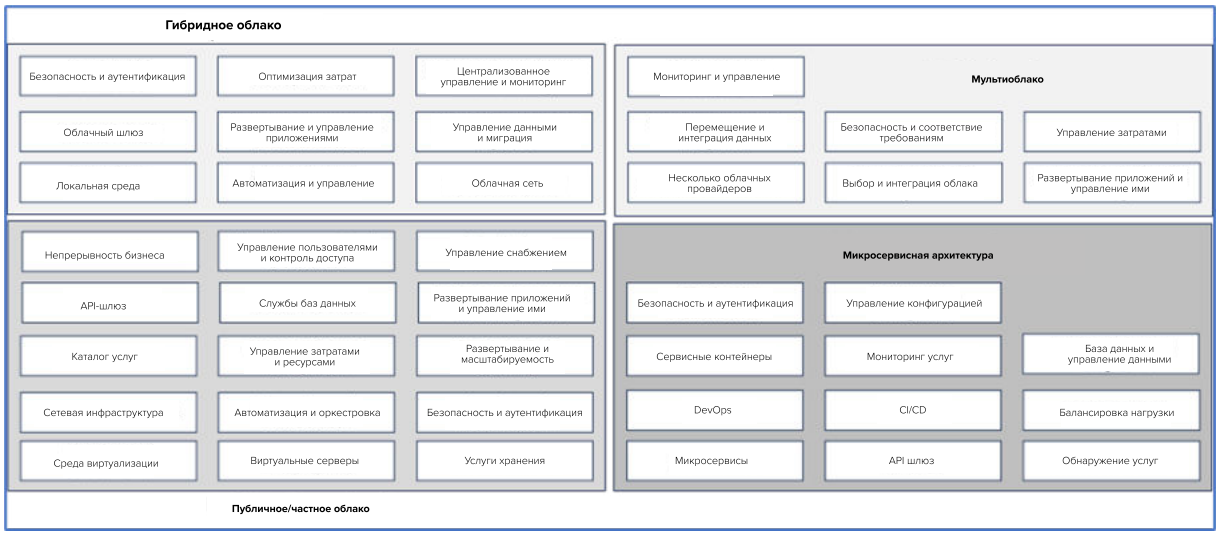
- ***Применение:*** поставщики SaaS предлагают различные типы программных приложений, включая электронную почту, обработку текстов, электронные таблицы, управление проектами, управление взаимоотношениями с клиентами (CRM), управление персоналом (HR) и многое другое.
- ***Доступ через Интернет:*** пользователи могут получать доступ к приложениям SaaS с любого устройства, подключенного к Интернету, с помощью веб-браузера или мобильного приложения, что обеспечивает гибкость и удобство.
- ***Мультитенантность:*** SaaS использует мультитенантную модель, позволяющую нескольким пользователям или организациям совместно использовать один и тот же экземпляр приложения, разделяя при этом данные и конфигурации.
- ***Обновления и обслуживание:*** поставщики SaaS занимаются обновлением и обслуживанием программного обеспечения. Пользователи автоматически получают доступ к последней версии, а такие задачи, как управление системой и исправления безопасности, выполняются поставщиком.
- ***Безопасность и управление данными:*** SaaS предоставляет различные функции для обеспечения безопасности данных, включая резервное копирование и восстановление данных, совместное использование данных и контроль доступа.
- ***Пользовательский интерфейс:*** приложения SaaS предоставляют пользовательский интерфейс (UI), позволяющий пользователям легко взаимодействовать и использовать приложение.
- ***Функции управления пользователями:*** включает функции, необходимые для управления учетными записями пользователей и разрешениями в программном приложении, предоставляемом поставщиком SaaS.
- ***Мониторинг услуг:*** в среде SaaS (программное обеспечение как услуга) мониторинг услуг включает в себя мониторинг и анализ состояния, производительности, доступности и моделей использования предоставляемых программных приложений для обеспечения рабочего состояния и оптимизации.
- ***Система выставления счетов:*** поставщики SaaS в основном используют модель оплаты на основе подписки. Пользователи платят ежемесячно или ежегодно за доступ к услуге и ее использование.

SaaS предлагает пользователям быстрый и удобный доступ к программному обеспечению и упрощает процесс покупки и управления программным обеспечением. Эта модель повышает эффективность как индивидуальных, так и деловых операций и может способствовать инновациям.

IV.5. Модели архитектуры исходя из типов развертывания облачных сервисов

Архитектуру облачных вычислений можно классифицировать по-разному, исходя из разных точек зрения, предлагая несколько типов, которые можно выбрать в соответствии с требованиями приложений и бизнеса. Ниже приведено введение в ключевые архитектуры облачных вычислений.

Рис. 13. Модели архитектуры исходя из типов развертывания облачных сервисов.



IV.5.1 Публичное/частное облако

Архитектура публичного облака основана на инфраструктуре, предоставляемой поставщиками облачных сервисов. Она позволяет разрабатывать, развертывать приложения и управлять ими с использованием различных сервисов и ресурсов. Архитектура частного облака предполагает создание выделенной облачной среды внутри организации. Она сочетает в себе требования безопасности и соответствия требованиям с гибкостью и эффективностью облачных вычислений.

Основными компонентами архитектуры публичного и частного облака являются следующие:

- ***Среда виртуализации:*** использует технологию виртуализации для разделения вычислительных ресурсов на виртуальные машины (ВМ) и контейнеры.
- ***Виртуальные серверы:*** экземпляры виртуальных машин (ВМ), на которых работают приложения и которые управляются в виртуализированной среде.
- ***Услуги хранения:*** предоставляет услуги хранения данных и управления ими, включая блочное хранилище, хранилище файлов и хранилище объектов.
- ***Сетевая инфраструктура:*** управляет сетевой связью между приложениями с использованием виртуальных сетей, балансировки нагрузки и брандмауэров.

- ***Автоматизация и управление:*** автоматизирует предоставление ресурсов, управление, масштабирование и управление задачами.
- ***Безопасность и аутентификация:*** реализует механизмы безопасности, такие как защита данных, контроль доступа и шифрование.
- ***Каталог услуг:*** определяет и предоставляет список доступных облачных сервисов и их характеристик.
- ***Управление пользователями и контроль доступа:*** реализует механизмы управления учетными записями пользователей, контроля доступа и аутентификации.
- ***Управление затратами и ресурсами:*** отслеживает и управляет использованием ресурсов, затратами и производительностью.
- ***Развертывание и масштабируемость:*** обеспечивает простое развертывание приложений и поддерживает горизонтальное и вертикальное масштабирование.
- ***API-шлюз:*** управляет взаимодействием между облачными службами и приложениями путем обработки вызовов API.
- ***Службы баз данных:*** предоставляет различные типы служб баз данных для управления и обработки данных.
- ***Развертывание и управление приложениями:*** предлагает инструменты и услуги для разработки, развертывания, управления и мониторинга приложений.
- ***Непрерывность бизнеса:*** обеспечивает непрерывность бизнеса за счет аварийного восстановления, резервного копирования и высокой доступности.

IV. 5.2 Гибридное облако

Гибридная облачная архитектура сочетает в себе локальные среды с общедоступными и частными облаками. Это позволяет организациям использовать сочетание ресурсов для удовлетворения своих потребностей.

Ключевые компоненты гибридной облачной архитектуры включают в себя:

- ***Локальная среда:*** включает существующие локальные центры обработки данных, серверы, сети и инфраструктуру.
- ***Публичное облако:*** использует ресурсы поставщиков общедоступных облаков.
- ***Облачная сеть:*** устанавливает безопасные и эффективные сетевые соединения между локальной и облачной средами.
- ***Облачный шлюз:*** управляет интеграцией данных и приложений между локальной и облачной средами.
- ***Развертывание и управление приложениями:*** развертывает приложения как в локальных, так и в облачных средах и автоматизирует управление ресурсами.
- ***Управление данными и миграция:*** управляет перемещением данных, синхронизацией, резервным копированием и восстановлением.
- ***Безопасность и аутентификация:*** обеспечивает безопасность между локальной и облачной средой.
- ***Оптимизация затрат:*** эффективно управляет использованием ресурсов, затратами и распределением бюджета.
- ***Централизованное управление и мониторинг:*** централизованно отслеживает и управляет ресурсами и состояниями приложений.

- ***Автоматизация и управление:*** оптимизирует управление ресурсами и развертывание приложений посредством автоматизированных рабочих процессов.

Гибридная облачная архитектура предлагает гибкую и безопасную среду за счет объединения локальных и облачных ресурсов для удовлетворения разнообразных требований.

IV.5.3 Мультиоблако

Мультиоблачная архитектура представляет собой стратегию одновременного использования нескольких облачных сред. Это предполагает объединение услуг и ресурсов от различных поставщиков облачных услуг или эффективное управление и использование распределенных облаков в разных регионах.

Ключевые компоненты мультиоблачной архитектуры следующие:

- ***Несколько поставщиков облачных услуг:*** в мультиоблачной архитектуре устанавливается интеграция с двумя или более различными поставщиками облачных услуг.
- ***Выбор и интеграция облака:*** возможность выбирать и интегрировать оптимальные облака, отвечающие потребностям организации, среди различных поставщиков облачных сервисов имеет решающее значение. Эффективная работа требует гармонизации сервисов, API, моделей данных и т.д. в различных облачных средах.
- ***Развертывание и управление приложениями:*** в мультиоблачной системе приложений необходимо распределять и управлять ими в нескольких облачных средах. Производительность и доступность приложений управляются с помощью балансировки нагрузки, автоматического масштабирования и управления.
- ***Перемещение и интеграция данных:*** для перемещения и интеграции данных в нескольких облаках необходима стратегия. Управление данными учитывает такие аспекты, как миграция данных, поток и совместимость.
- ***Безопасность и соответствие требованиям:*** соблюдение различных политик и правил безопасности важно в мультиоблачной среде. Для обеспечения безопасности реализуются механизмы безопасности, такие как защита данных, контроль доступа и шифрование.
- ***Управление затратами:*** необходимо понимание моделей затрат каждого поставщика облачных услуг и эффективное управление затратами. Анализ затрат, распределение бюджета и оптимизация затрат минимизируют расходы и максимизируют выгоды.
- ***Мониторинг и управление:*** в мультиоблачной архитектуре требуется мониторинг и управление состоянием и производительностью нескольких облачных сред. Инструменты или службы централизованного мониторинга отслеживают рабочее состояние и обнаруживают проблемы на ранней стадии.

Мультиоблачная архитектура обеспечивает стратегию гармонизации нескольких облачных сред для обеспечения гибкой и эффективной работы в соответствии с бизнес-требованиями организации.

IV.5.4 Периферийное облако

Архитектура периферийного облака представляет собой модель, в которой ресурсы облачных вычислений предоставляются в регионах, близких к периферийным устройствам. Он предназначен для приложений, требующих быстрой обработки данных и ответов в режиме реального времени.

Ключевые компоненты периферийной облачной архитектуры следующие:

- ***Периферийные устройства:*** основные компоненты периферийной облачной архитектуры, включая датчики, камеры, коммутаторы и подобные устройства. Они собирают и передают данные в режиме реального времени.
- ***Периферийный шлюз:*** расположенный между периферийными устройствами и облаком, периферийный шлюз собирает и предварительно обрабатывает данные перед отправкой их в облако. Он выполняет такие функции, как сжатие, шифрование и фильтрация данных.
- ***Периферийный сервер:*** выполняет локальную обработку и анализ данных. Выступая в качестве промежуточного уровня между периферийными устройствами и периферийным облаком, он поддерживает приложения, требующие реагирования в реальном времени.
- ***Облачные ресурсы:*** в архитектуре периферийного облака центральное облако выполняет дополнительную обработку, анализ и долгосрочное хранение данных. Центральное облако выполняет задачи, которые не могут выполнить периферийные устройства и серверы.
- ***Периферийная сеть:*** требуется стабильное сетевое соединение между периферийными устройствами, шлюзами, серверами и облаком в архитектуре периферийного облака. Крайне важно иметь сеть, поддерживающую быструю передачу данных и безопасную связь.
- ***Потоковая передача и анализ данных:*** платформы потоковой передачи и анализа данных в реальном времени обрабатывают и анализируют данные, собранные на периферии, в режиме реального времени. Это позволяет создавать приложения реагирования в режиме реального времени.
- ***Безопасность и аутентификация:*** архитектура периферийного облака должна реализовывать механизмы безопасности и методы аутентификации для обеспечения безопасности данных и целостности устройства.
- ***Бизнес-приложения:*** приложения, разработанные для периферийной облачной архитектуры, предоставляют такие функции, как анализ в режиме реального времени, прогнозные модели, автоматические ответы и поддержка принятия решений.

Периферийная облачная архитектура играет решающую роль в сферах, требующих быстрой обработки данных и реагирования, позволяя создавать приложения реального времени и управлять ими посредством комбинации этих компонентов.

V.5.5 Микросервисная архитектура

Архитектура микросервисов — это архитектурный шаблон, который разлагает программные системы на небольшие независимые функциональные единицы. Каждый микросервис можно развертывать, масштабировать и управлять им индивидуально, он может использовать различные технологические стеки и независимые базы данных.

Ключевые компоненты архитектуры микросервисов следующие:

- ***Микросервисы:*** основными компонентами архитектуры микросервисов являются отдельные микросервисы, выполняющие независимые функции. Каждый микросервис реализует определенные бизнес-функции и разрабатывается, развертывается и управляется в небольших масштабах.
- ***API-шлюз:*** управляет связью между клиентами и микросервисами. API-шлюз направляет клиентские запросы в соответствующие микросервисы и обрабатывает аутентификацию, авторизацию, ведение журналов, балансировку нагрузки и многое другое.
- ***Обнаружение сервисов:*** этот механизм отслеживает и обнаруживает динамическое расположение микросервисов. Система обнаружения сервисов поддерживает регистрацию, обновление и запросы микросервисов.
- ***DevOps:*** (сокр. от «Development and Operations»), представляет собой культуру, философию и методологию, которые интегрируют процессы разработки и развертывания программного обеспечения. Он улучшает сотрудничество между командами разработки и эксплуатации и направлен на повышение частоты и качества разработки и развертывания программного обеспечения, чтобы быстрее и надежнее реагировать на потребности бизнеса.
- ***Балансировка нагрузки:*** распределяет трафик между несколькими экземплярами, чтобы равномерно распределить нагрузку каждого микросервиса. Такая оптимизация минимизирует время отклика и повышает доступность.
- ***Мониторинг сервисов:*** отслеживает производительность и доступность каждого микросервиса, собирает журналы, выявляет и устраняет проблемы. Мониторинг является важнейшим элементом поддержки эксплуатации и технического обслуживания.
- ***Контейнеры сервисов:*** микросервисы выполняются в изолированных контейнерных средах, что обеспечивает изоляцию и масштабируемость между службами. Такой подход позволяет использовать разные языки и технологии.
- ***База данных и управление данными:*** каждый микросервис может иметь собственную базу данных по мере необходимости. Такие методы, как источник событий и шаблоны CQRS, можно использовать для управления данными и обеспечения согласованности.
- ***Безопасность и аутентификация:*** между микросервисами реализуются механизмы безопасности, такие как аутентификация и авторизация. Защита данных и сетевая безопасность также являются важными факторами.
- ***Управление конфигурацией:*** микросервисы работают с использованием конфигураций и переменных среды. Для управления конфигурациями каждой службы используется централизованная система управления конфигурациями.

- ***CI/CD (непрерывная интеграция/непрерывное развертывание):*** архитектура микросервисов использует конвейеры CI/CD для автоматизированной разработки и развертывания, поддерживая быстрое развертывание и интеграцию.

Микросервисная архитектура обеспечивает более быструю и эффективную разработку и эксплуатацию приложений благодаря модульному дизайну и гибкой реализации.

IV.5.6 Бессерверная архитектура

Бессерверная архитектура — это модель облачных вычислений, которая сводит к минимуму управление сервером для разработки и развертывания приложений. Разработчики освобождаются от бремени управления сервером, а модель сосредоточена на выполнении функций, управляемых событиями.

Ключевые элементы бессерверной архитектуры:

- ***Функции:*** в бессерверной архитектуре функциональность приложения разделена на небольшие блоки, называемые функциями. Функции автоматически запускаются событиями, выполняют необходимые вычисления и возвращают результаты.
- ***Триггеры событий:*** механизмы, определяющие события, активирующие функции. События могут быть вызваны изменениями в состоянии приложения или внешними входами. Примеры включают HTTP-запросы, изменения базы данных и таймеры.
- ***Облачные сервисы:*** облачные сервисы в бессерверной архитектуре управляют выполнением функций и динамически распределяют ресурсы по мере необходимости. Это избавляет разработчиков от необходимости управлять серверами, масштабировать и обслуживать их.
- ***Функциональные контейнеры:*** изолированные контейнерные среды, используемые для выполнения каждой функции. Они обеспечивают изоляцию и безопасность между выполнением функций, а также упрощают масштабирование и управление.
- ***Службы хранения данных и базы данных:*** службы хранения данных и базы данных необходимы для хранения и извлечения данных для приложений. Это позволяет функциям получать доступ к данным и обрабатывать их.
- ***API-шлюз:*** интерфейс, который обрабатывает внешние запросы и вызывает функции. Он преобразует клиентские запросы в события для запуска функций и возвращает результаты функций клиентам.
- ***Безопасность и аутентификация:*** безопасность остается важной в бессерверной среде. Механизмы контроля доступа, шифрования данных, а также аутентификации и авторизации обеспечивают безопасность данных и функций.
- ***Ведение журнала и мониторинг:*** отслеживает выполнение и производительность функций, собирает журналы для отладки и повышения производительности.
- ***Настройка конфигурации и среды:*** бессерверные приложения работают на основе переменных среды и информации о конфигурации, что позволяет разработчикам настраивать поведение функций и интегрироваться с внешними службами.

- ***Автоматическое масштабирование:*** бессерверные среды автоматически масштабируют функции в зависимости от объема запросов, оптимизируя использование ресурсов.

Бессерверная архитектура позволяет разработчикам сосредоточиться на выполнении кода, обеспечивая обработку, управляемую событиями, и гибкую масштабируемость. Это может быть полезно в различных сценариях разработки и развертывания приложений.

IV.6. Детальные технические компоненты облачной архитектуры

Компоненты эталонной облачной архитектуры представляют собой фундаментальные принципы и элементы, используемые при проектировании и создании сервисов в среде облачных вычислений. Эти компоненты архитектуры необходимо учитывать в процессе проектирования и внедрения облака. Объединив эти элементы, можно реализовать эффективные и стабильные облачные сервисы и приложения.

IV.6.1 Облачная безопасность и управление авторизацией

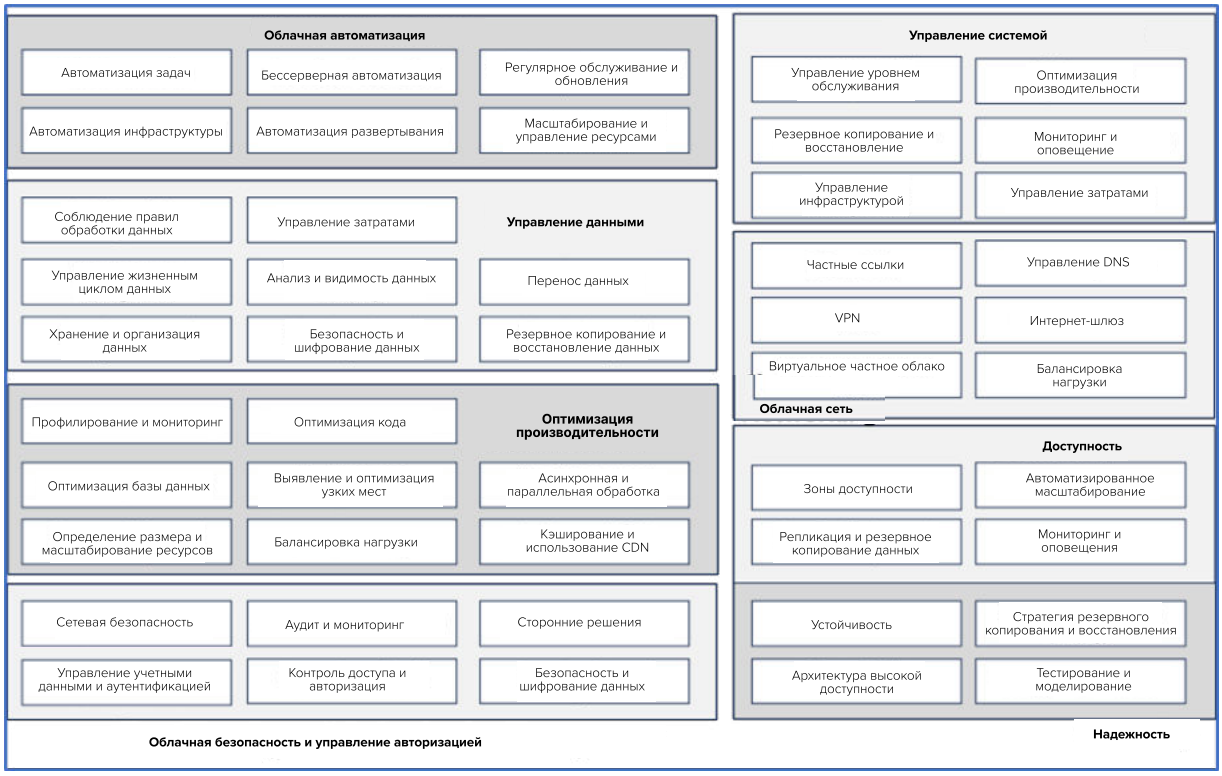
Облачная безопасность и управление авторизацией необходимы для защиты данных и управления разрешениями на доступ в среде облачных вычислений. Для эффективного управления безопасностью и авторизацией в облачной среде необходимо включить следующие функции:

- ***Управление учетными данными и аутентификацией:*** защищает доступ к данным пользователей и ресурсам с помощью политик надежных паролей. Многофакторная аутентификация (MFA) обеспечивает дополнительный уровень безопасности. Управление доступом на основе ролей реализовано в соответствии с принципом наименьших привилегий.
- ***Контроль доступа и назначение авторизации:*** эффективное управление пользователями, группами и ролями для предоставления только необходимых разрешений. Применение детальных политик контроля доступа ограничивает доступ к необходимым задачам. Улучшает контроль за удаленным доступом и доступом через API.
- ***Безопасность и шифрование данных:*** конфиденциальные данные защищены соответствующими методами шифрования. Шифрование используется во время передачи данных и статического/динамического хранения. Строгое управление ключами и их ротация усиливают защиту данных.
- ***Сетевая безопасность:*** настраивает виртуальные сети и брандмауэры для создания групп безопасности и сетевых политик. Использует механизмы защиты сети, такие как защита от DDoS-атак.
- ***Аудит и мониторинг:*** отслеживает действия системы посредством регистрации событий и мониторинга, обнаруживая аномальные действия. Регулярно просматривает журналы аудита для реагирования и расследования инцидентов безопасности.
- ***Сторонние решения:*** используются инструменты безопасности, предоставляемые поставщиками облачных услуг, и сторонние решения безопасности для дополнительных функций безопасности. Повышает уровень безопасности с помощью сканирования уязвимостей, анализа угроз и многого другого.

- ***Соответствие нормативным требованиям:*** соответствует отраслевым нормам и законодательным требованиям, обеспечивая при этом защиту данных и конфиденциальность.

Соблюдение этих методов управления безопасностью и авторизацией обеспечивает безопасность данных и ресурсов в облачной среде и сводит к минимуму уязвимости в инфраструктуре и приложениях.

Рис. 14. Детальные технические компоненты облачной архитектуры.



IV.6.2 Надежность и доступность

Надежность и доступность облака являются важными концепциями облачных вычислений, обеспечивающими стабильность системы и постоянную доступность.

- ***Надежность:*** в облачной среде надежность означает, что система работает нормально и может надлежащим образом восстанавливаться после сбоев или проблем. Для повышения надежности облачных сервисов рассматриваются следующие подходы:
  - *Устойчивость:* способность системы сохранять высокую надежность во время сбоев или проблемных ситуаций и быстро восстанавливаться. Повышает отказоустойчивость за счет распределения серверов по нескольким регионам или создания автоматизированных процессов восстановления.
  - *Стратегия резервного копирования и восстановления:* регулярное резервное копирование данных и реализация эффективных стратегий восстановления в случае потери данных.
  - *Архитектура высокой доступности:* для обеспечения высокой доступности используются такие архитектурные шаблоны, как балансировка нагрузки, автоматическое масштабирование, репликация и т.д.

- *Архитектура высокой доступности:* для обеспечения высокой доступности используются такие архитектурные шаблоны, как балансировка нагрузки, автоматическое масштабирование, репликация и т.д.
- *Тестирование и моделирование:* моделирование сценариев сбоя и проведение регулярных тестов восстановления для обеспечения надежности.

- ***Доступность:*** в облачной среде доступность означает способность пользователей и приложений получать доступ к сервисам и ресурсам, когда это необходимо. Для повышения доступности в облачной среде актуальны следующие подходы:
  - *Зоны доступности:* поставщики облачных услуг предлагают географически распределенные зоны доступности, чтобы гарантировать бесперебойную работу сервисов даже в случае сбоев.
  - *Автоматическое масштабирование:* ресурсы автоматически масштабируются (в сторону увеличения или уменьшения) в зависимости от колебаний трафика, сохраняя доступность.
  - *Репликация и резервное копирование данных:* данные реплицируются и создаются их резервные копии в нескольких местах, чтобы предотвратить потерю данных и обеспечить доступность.
  - ***Мониторинг и оповещения:*** мониторинг состояния системы и приложений позволяет быстро оповещать и реагировать на потенциальные проблемы.

Надежность и доступность облака играют решающую роль в обеспечении непрерывности бизнеса и повышении удовлетворенности пользователей. Для достижения этой цели поставщики облачных услуг предлагают различные функции безопасности и доступности, а пользователи могут внести свой вклад, проектируя и настраивая облачную среду соответствующим образом для поддержания надежности и доступности.

IV.6.3 Оптимизация производительности

Оптимизация производительности облака — это процесс повышения производительности приложений и сервисов в облачной среде с целью улучшения пользовательского опыта и эффективного использования ресурсов. Чтобы оптимизировать производительность облака, следует учитывать несколько ключевых факторов и лучших практик:

- ***Определение размера и масштабирование ресурсов:*** при необходимости настройте размер виртуальных машин или контейнеров для повышения производительности. Используйте настройки автоматического масштабирования для динамического расширения или сокращения ресурсов в зависимости от колебаний трафика.
- ***Балансировка нагрузки:*** используйте балансировщики нагрузки для распределения трафика между несколькими серверами или ресурсами, обеспечивая сбалансированное время отклика и повышенную доступность.
- **Кэширование и использование CDN:** используйте механизмы кэширования для хранения часто используемых данных или контента, сокращая время отклика. Используйте сети доставки контента (CDN) для регионального кэширования контента для более быстрого реагирования на запросы пользователей.

- ***Оптимизация базы данных:*** повышение производительности базы данных с помощью таких методов, как индексирование и секционирование. Выполните оптимизацию запросов и настройку индекса для повышения скорости получения данных.
- ***Выявление и оптимизация узких мест:*** выявление и устранение узких мест в производительности приложения. Устраните узкие места, такие как запросы к базе данных или сетевые подключения.
- ***Асинхронная и параллельная обработка:*** используйте асинхронное программирование и параллельную обработку для эффективного выполнения задач, сокращая время отклика.
- ***Профилирование и мониторинг:*** мониторинг производительности приложений и системы с помощью инструментов профилирования для выявления узких мест и постоянной оценки производительности.
- ***Оптимизация кода:*** напишите эффективный код и улучшите алгоритмы для оптимизации времени обработки и использования ресурсов.

Оптимизация производительности облака играет решающую роль в повышении эффективности приложений и удобства пользователей. Учитывая оптимизацию с различных аспектов, таких как использование ресурсов, обработка данных и архитектура приложений, а также путем постоянного мониторинга и корректировки, вы можете поддерживать оптимальную производительность.

IV.6.4 Облачная сеть

Облачные сети относятся к инфраструктуре и технологиям, которые обеспечивают связь между приложениями, сервисами и ресурсами в среде облачных вычислений. Они обеспечивают подключение пользователей, безопасную передачу данных и являются жизненно важным компонентом облачной экосистемы.

Различные сетевые концепции и функции облачных сетей включают в себя:

- ***Виртуальное частное облако (VPC):*** создает изолированные сетевые среды с использованием VPC для защиты и управления сетевым трафиком между ресурсами.
- ***Балансировка нагрузки:*** использует балансировщики нагрузки для распределения трафика между несколькими серверами или ресурсами, оптимизируя время отклика и доступность.
- ***Брандмауэры и группы безопасности:*** настраивает брандмауэры и группы безопасности для повышения сетевой безопасности и управления контролем доступа.
- ***VPN (виртуальная частная сеть):*** создает виртуальную частную сеть между облачными сетями и локальными сетями для безопасных соединений.
- ***Интернет-шлюз:*** настраивает шлюзы для управления и защиты связи между Интернетом и облачной сетью.
- ***Управление DNS:*** управляет внутренней и внешней системой доменных имен (DNS) для разрешения и управления доменными именами в IP-адресах.

- ***Частные каналы:*** устанавливает выделенные сетевые соединения между поставщиком облачных услуг и вашей сетью для повышения скорости и безопасности передачи данных.
- ***Маршрутизация BGP:*** использует маршрутизацию по протоколу пограничного шлюза (BGP) для управления эффективной передачей данных между несколькими сетями.
- ***Поддержка IPv6:*** использует адресацию IPv6 для выделения большего количества IP-адресов и обеспечения масштабируемости сети.

Облачные сети необходимы для управления передачей данных, взаимодействием приложений и безопасностью в облачной среде. Эффективная настройка и управление облачными сетями имеет важное значение для обеспечения безопасных соединений и оптимизации производительности.

IV.6.5 Управление облачными данными

Управление облачными данными — это процессы хранения, защиты, анализа, резервного копирования и управления данными в облачной среде. Оно обеспечивает безопасность, доступность и эффективность данных для достижения бизнес-целей.

Ключевые подходы и лучшие практики управления облачными данными включают:

- ***Хранение и организация данных:*** используйте облачное хранилище для безопасного и эффективного хранения данных. Можно использовать такие сервисы, как базы данных и объектное хранилище. Организуйте данные в подходящих форматах для удобства запросов и анализа.
- ***Безопасность и шифрование данных:*** шифруйте конфиденциальные данные при их хранении и во время передачи, добавляя дополнительный уровень безопасности. Контролируйте доступ и управляйте разрешениями для данных.
- ***Резервное копирование и восстановление данных:*** регулярно создавайте резервные копии данных, чтобы подготовиться к возможным сценариям потери данных. Разработайте стратегии и процессы восстановления для быстрого восстановления данных из резервных копий.
- ***Управление жизненным циклом данных:*** установите политики хранения, хранения и удаления данных в зависимости от этапов их жизненного цикла.
- ***Анализ и наглядность данных:*** используйте облачные инструменты анализа данных, чтобы извлечь из данных ценность и получить ценную информацию. Отслеживайте состояние данных и тенденции с помощью информационных панелей и визуализации.
- ***Миграция данных:*** спланируйте и выполните миграцию данных из локальных систем в облако. Поддерживайте согласованность и стабильность данных во время миграции.
- ***Соответствие правилам обработки данных:*** соблюдайте правила использования данных и законодательные требования даже в облачной среде.
- Управление затратами: оценка и оптимизация данных в целях управления затратами на управление данными.

Эффективное управление облачными данными играет решающую роль на протяжении всего жизненного цикла данных. Правильное управление усиливает защиту, анализ, прозрачность и доступность данных, способствуя улучшению бизнес-результатов.

IV.6.6 Облачная автоматизация

Под облачной автоматизацией понимаются автоматизация задач, подготовка, развертывание, управление и многое другое в облачной среде для эффективного управления системными операциями и оптимизации использования ресурсов. Автоматизируя повторяющиеся и громоздкие задачи, облачная автоматизация повышает производительность разработчиков и операторов, одновременно снижая сложность управления инфраструктурой. Ниже приведены ключевые аспекты и некоторые лучшие практики облачной автоматизации:

- ***Автоматизация инфраструктуры:*** автоматизируйте предоставление и управление компонентами облачной инфраструктуры, такими как виртуальные машины, контейнеры и сети. Определите инфраструктуру как код и используйте инструменты автоматизации (например, Terraform, AWS CloudFormation) для автоматической настройки сред.
- ***Автоматизация развертывания:*** автоматизируйте процесс развертывания и обновления приложений в облаке. Интегрируйтесь с конвейерами CI/CD для автоматического создания, тестирования и развертывания изменений кода.
- ***Масштабирование и управление ресурсами:*** автоматическое масштабирование ресурсов в зависимости от увеличения трафика для поддержания производительности и экономии затрат. Отслеживайте использование ресурсов и настраивайте триггеры масштабирования для автоматической корректировки ресурсов.
- ***Автоматизация задач:*** автоматизируйте повторяющиеся задачи с помощью сценариев или инструментов автоматизации. Например, автоматизируйте такие задачи, как резервное копирование, управление журналами и аудит безопасности.
- ***Бессерверная автоматизация:*** используйте бессерверную архитектуру для автоматизации выполнения кода. Функции автоматически масштабируют среду выполнения и осуществляют управление ею.
- ***Регулярное обслуживание и обновления:*** автоматизируйте регулярные задачи, такие как исправление ОС, обновления безопасности и обновления приложений, чтобы поддерживать системы в актуальном состоянии. Автоматизация облака повышает операционную эффективность и экономит время и усилия за счет автоматизации управления инфраструктурой и приложениями. Однако тщательное тестирование и проверка необходимы при внедрении автоматизации для обеспечения точности и стабильности.

Использование облачной автоматизации повышает эффективность управления системой, позволяя автоматически управлять инфраструктурой и приложениями, тем самым экономя время и усилия. Однако при внедрении автоматизации необходимы достаточные тесты и проверки для обеспечения точности и надежности.

IV.6.7 Управление и мониторинг облака

Управление облаком и мониторинг включают эффективное управление ресурсами и услугами в облачной среде и мониторинг производительности для поддержания стабильности и доступности. Из-за разнообразия и гибкости ресурсов в облаке крайне важно эффективное управление и мониторинг.

Подходы и лучшие практики управления облаком и мониторинга включают в себя:

- ***Управление инфраструктурой:*** используйте инструменты автоматизации (например, Terraform, Ansible) для предоставления облачных ресурсов и управления ими. Определите инфраструктуру как код для контроля версий и воспроизводимости.
- ***Управление затратами:*** отслеживайте затраты на облачные ресурсы и используйте инструменты отслеживания затрат для управления бюджетами. Предотвратите ненужное использование ресурсов и поддерживайте их эффективное распределение.
- ***Управление безопасностью:*** Повысьте безопасность облачных ресурсов путем настройки контроля доступа, групп безопасности и брандмауэров. Используйте сканирование уязвимостей и журналы аудита для предотвращения инцидентов безопасности и реагирования на них.
- ***Резервное копирование и восстановление:*** настройте регулярное резервное копирование данных и подготовьте стратегии восстановления на случай потери данных. Поддерживайте тестирование и процессы для быстрого восстановления данных резервных копий.
- ***Мониторинг и оповещение:*** настройте инструменты мониторинга для мониторинга производительности ресурсов и приложений и раннего обнаружения потенциальных проблем. Настройте оповещения и уведомления для немедленного реагирования на проблемы.
- ***Оптимизация производительности:*** Анализируйте использование ресурсов, время отклика и трафик для выявления и оптимизации узких мест в производительности. Используйте автоматическое масштабирование и изменение размера ресурсов для повышения производительности.
- ***Управление уровнем обслуживания:*** отслеживайте соглашения об уровне услуг (SLA) и следите за тем, чтобы поставщик услуг соблюдал соглашения SLA. Управляйте временем и процессами восстановления во время инцидентов.

Управление и мониторинг облака играют решающую роль в поддержании стабильности, доступности и выполнении бизнес-требований. Эффективное управление и мониторинг позволяют предотвращать и быстро решать системные проблемы, повышая удобство работы пользователей и сокращая затраты.

IV.7. Рекомендации по внедрению облачных вычислений для государственного управления

Когда органы государственного управления рассматривают возможность внедрения облака, они должны сначала оценить существующие информационные системы и

организацию управления. Благодаря этому они смогут четко определить цели внедрения облака и максимизировать преимущества его внедрения.

Команда проекта по внедрению облака должна сначала оценить технические факторы существующих локальных информационных систем. Техническая оценка нацелена на аппаратное обеспечение, программное обеспечение, базы данных, сеть и все аспекты ИТ-инфраструктуры и приложений. Посредством такой оценки можно диагностировать экономию затрат, виртуализацию, совместное использование ИТ-ресурсов, масштабируемость, гибкость обслуживания и потенциал автоматизации.

Во-вторых, команда проекта должна оценить уровень обеспеченности ИТ-ресурсами, управление ИТ и текущий статус процессов предоставления ИТ-ресурсов. Посредством таких оценок можно диагностировать потенциал улучшения уровня предоставления ИТ-услуг бизнес-организациям, которые являются потребителями ИТ, а также уровень ИТ-операций и управления.

В-третьих, команда проекта должна оценить структуру, роли и обязанности, стиль управления, рабочую среду, цели и статус обучения ИТ-организации. Это поможет определить, возможен ли переход от ИТ-организации, специализирующейся на отдельных технологиях, к сервисно-ориентированной и бизнес-ориентированной ИТ-организации.

В-четвертых, команда проекта должна оценить потребность бизнес-организации в ИТ-услугах и текущий уровень реагирования ИТ-организации. Проанализировав, можно ли преобразовать управление ИТ в модель, в которой распределение бюджета и расходы производятся на основе спроса и использования ИТ в масштабе всего предприятия, команда может определить целесообразность.

Посредством таких оценок организация должна принять решение в области внедрения облака, методах и формах облака (IaaS, PaaS, SaaS). Тип облака, которое будет принято, может варьироваться в зависимости от таких факторов, как характеристики систем, которыми обладает организация, бюджет, чувствительность к производительности, соответствие требованиям безопасности и другие соображения.

IV.7.1 Миграция на IaaS

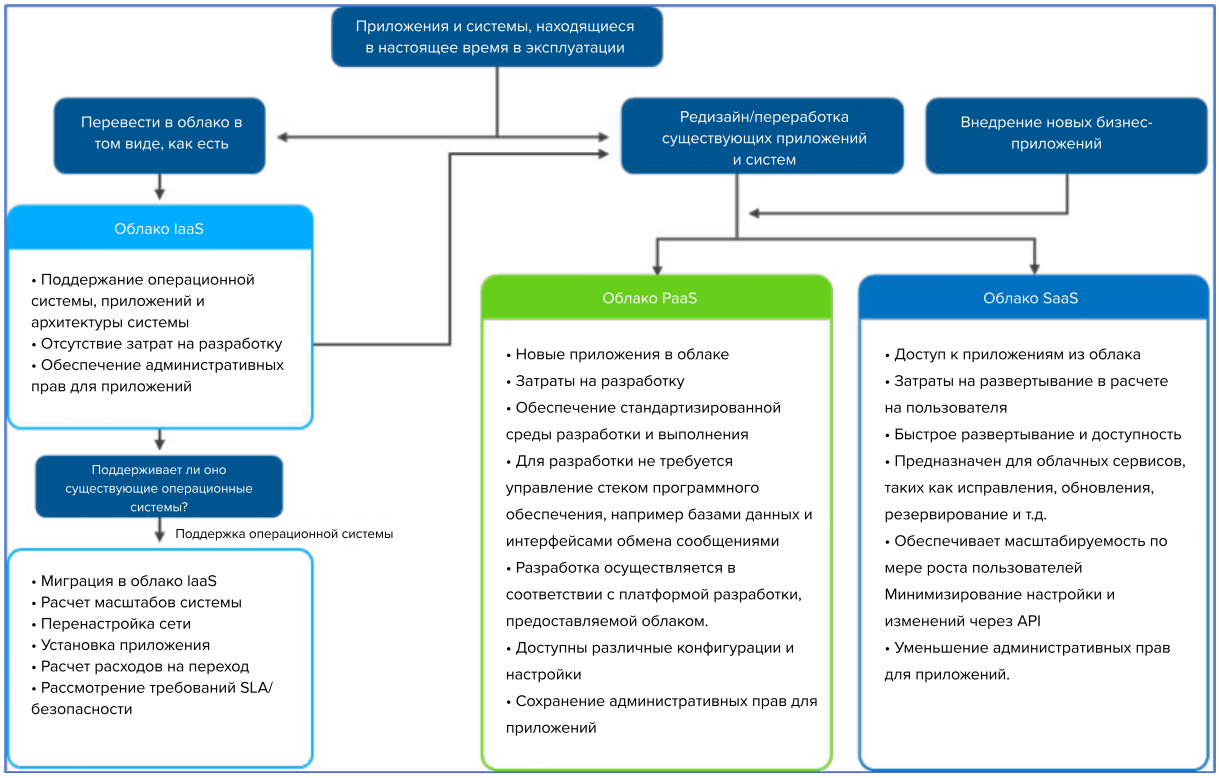
В зависимости от ситуации государственных учреждений и системных условий проводится оценка возможности принятия инфраструктуры как услуги (IaaS) для целевых систем. Если результаты оценки показывают, что облако IaaS не подходит или требуется доработка, редизайн или внедрение новых приложений, рассматривается возможность внедрения облака «Программное обеспечение как услуга» (SaaS) или «Платформа как услуга» (PaaS).

Критерии оценки целесообразности внедрения услуг облачной инфраструктуры следующие:

- Поддерживаются ли облачные службы текущими операционными системами предприятия?

- Если необходимо обновление ОС, будет ли оно совместимо с существующими приложениями или базами данных?
- Сложно ли изменить бизнес-процессы, требующие максимального сохранения существующей системы?
- Есть ли какие-либо проблемы с лицензированием приложений из-за перехода в облако?

Рис. 15: Критерии и характеристики определения типа облака



продолжать использовать корпоративные базы данных и другие компоненты без серьезных проблем с совместимостью, выбор «Инфраструктура как услуга» (IaaS) действительно может стать оптимальным решением. При выборе IaaS необходимо предпринять несколько шагов, включая определение размера системы, настройку сети, установку приложений, оценку затрат на миграцию, проверку соглашений об уровне услуг (SLA) и выполнение требований безопасности.

После завершения предмиграционной подготовки происходит процесс миграции систем и данных, за которым следует проверка целостности переносимых систем и данных. После завершения миграции государственное учреждение может начать пилотные операции в облачной среде для мониторинга и проверки различных аспектов. Впоследствии государственное учреждение приступает к работе по стабилизации услуг, обеспечивая бесперебойную работу операций, мониторинга и контроля в нормальном состоянии.

IV.7.2 Миграция с использованием PaaS

Когда государственные учреждения не могут использовать услуги облачной инфраструктуры, они могут разработать новое программное обеспечение на основе

PaaS (платформа как услуга). Можно разработать индивидуальное SaaS (программное обеспечение как услуга), максимально учитывая требования пользователей государственных учреждений. Альтернативно существующие приложения могут быть реорганизованы на основе PaaS. Поставщики облачных услуг предлагают необходимую среду для разработки SaaS в форме PaaS, включая среды разработки и эксплуатации, базы данных, серверы веб-приложений (WAS), обмен сообщениями и многое другое. При использовании PaaS требуются время и затраты на разработку, и разработка должна продолжаться с использованием среды разработки, предоставляемой PaaS. После разработки может возникнуть зависимость от среды PaaS поставщика облачных услуг, поэтому руководителю государственного учреждения следует помнить об этом.

В последнее время при разработке SaaS с использованием PaaS предпочтение отдается облачной архитектуре. В облачном подходе единый SaaS состоит из комбинации нескольких независимых микросервисов и использует контейнеры в качестве среды выполнения для микросервисов. Поставщикам облачных услуг требуются инструменты для управления многочисленными контейнерами. Кроме того, для непрерывного развертывания приложений необходима функциональность CI/CD (непрерывная интеграция/непрерывное развертывание), а также такие инструменты, как DevOps, чтобы обеспечить совместную работу разработки и эксплуатации в рамках одной организации. SaaS, разработанный в облачном формате, может обеспечить гораздо более широкие возможности балансировки нагрузки и преимущества плавного обновления SaaS.

IV.7.3 Переход на SaaS

Это форма внедрения услуг SaaS (программное обеспечение как услуга), предоставляемых поставщиками услуг SaaS. В этом случае обязательным условием является наличие на рынке SaaS-предложений, подходящих для нужд государственных учреждений. Если предложения SaaS не полностью отвечают требованиям государственных учреждений, может оказаться необходимым запросить настройку определенных приложений у поставщика SaaS. Среди форм внедрения облака это наиболее быстрый метод развертывания и использования. При использовании SaaS возникают затраты на внедрение с учетом количества пользователей, а также возникает проблема снижения полномочий по управлению приложениями. Такие проблемы, как масштабирование ресурсов из-за роста числа пользователей, изменения или обновления приложений, решаются под ответственность поставщика SaaS. Таким образом, любые изменения или обновления SaaS должны выполняться после достаточной предварительной консультации между пользователями услуг и поставщиком. Контроль за качеством и управлением уровнем сервиса SaaS может осуществляться должностными лицами государственных учреждений посредством соглашений SLA (Соглашений об уровне услуг).

IV.7.4 Миграция в гибридное облако

Если группа по внедрению облака решит оставить некоторые системы локальными по таким причинам, как сложность системы, конфиденциальность данных или вопросы стоимости, они могут рассмотреть возможность внедрения решения гибридного облака. В таких случаях важно обеспечить плавную интеграцию и согласованный контроль между

общедоступным облаком и локальными системами. Некоторые поставщики облачных услуг даже предлагают интегрированные консоли управления для локальных и общедоступных облачных ресурсов, специально разработанные для развертывания гибридного облака. Кроме того, они предоставляют функции для унифицированного управления сетями между виртуальными машинами или контейнерами в публичном облаке и локальных системах.

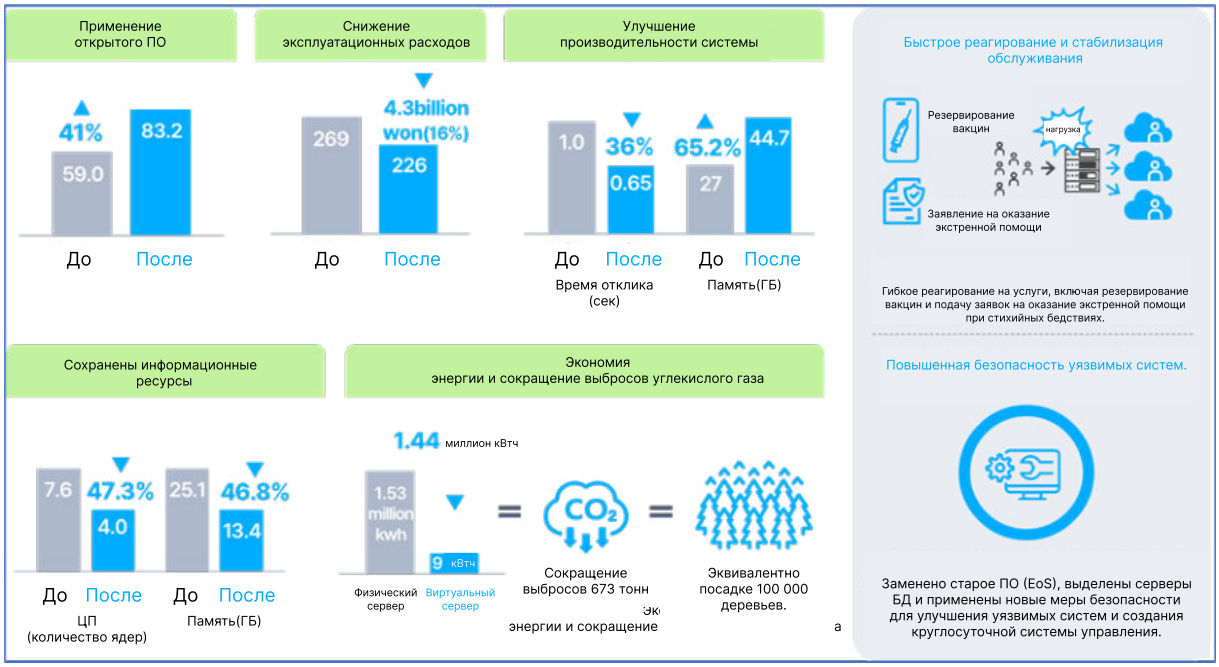
IV.8. Практические примеры и результаты внедрения облачных технологий в государственных учреждениях

IV.8.1 Внедрение IaaS

Под руководством Министерства государственного управления и безопасности Южной Кореи в период с 2020 по 2021 год был реализован проект по переносу 302 систем, которыми управляют более 30 государственных учреждений, в облако. Каждое учреждение перенесло системы, управление которыми ранее осуществлялось индивидуально в своих центрах обработки данных, в G-Cloud (облако, управляемое Государственным интегрированным центром обработки данных) для достижения системной интеграции и увеличения времени безотказной работы системы за счет использования виртуализированных серверов, сетей и ресурсов хранения.

В результате каждое учреждение смогло сэкономить примерно 16% эксплуатационных расходов, которые они несли при индивидуальном управлении своими центрами обработки данных. В среднем время отклика системы улучшилось примерно на 36%, а использование системных ресурсов сократилось примерно на 40%. Это привело к ежегодной экономии энергии в размере 1,44 млн. кВтч, что, по оценкам, эквивалентно сокращению выбросов на 673 тонны углекислого газа.

Рис. 16. Эффекты внедрения IaaS государственными учреждениями

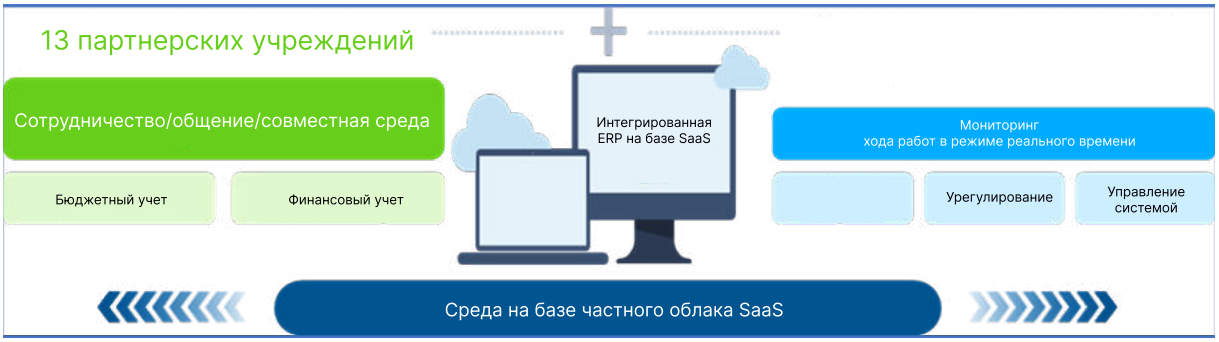


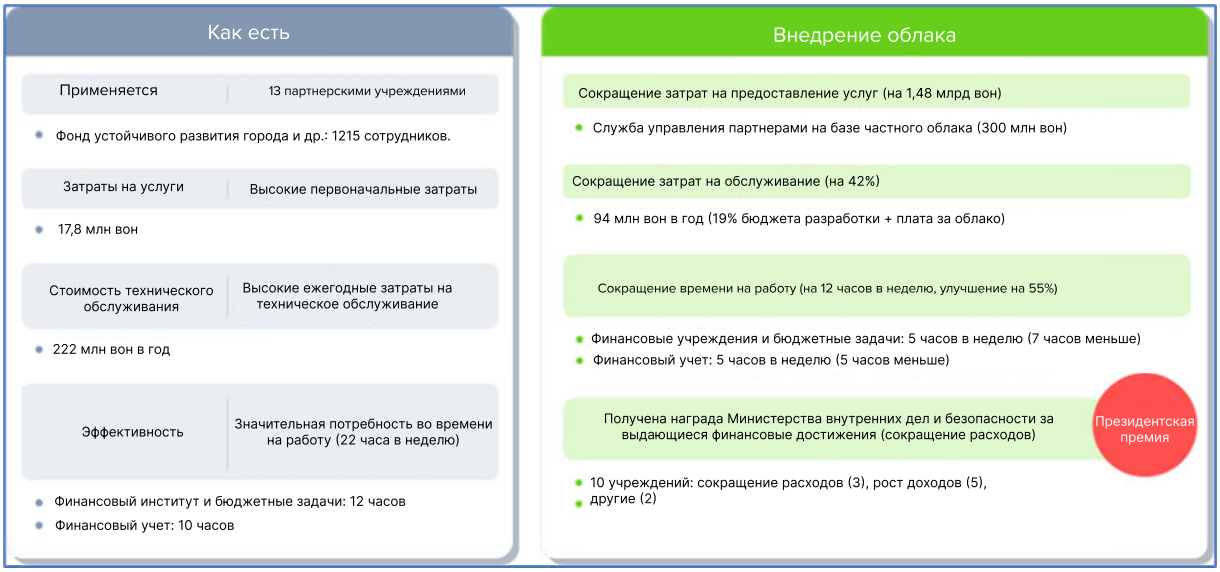
IV.8.2 Внедрение PaaS/SaaS

Город Сувон стал первым местным органом власти в Южной Корее, который создал интегрированные службы бюджетного учета с 13 партнерскими агентств, использующими частное облако SaaS. Город Сувон создал облачную информационную среду для оцифровки данных бюджетного учета и интеграции внутренних и внешних систем. Раньше в городе Сувон значительное количество времени (22 часа в неделю) уделялось обработке бюджета партнерских агентств, и затраты на обслуживание были высокими. Для решения этих вопросов в Сувоне разработана и эксплуатируется SaaS-система управления финансовым учетом в интегрированном формате с участием 13 партнерских агентств.

В результате внедрения облачных решений SaaS город Сувон смог сократить рабочую силу, необходимую для процессов финансового учета, на 50% и снизить эксплуатационные расходы на 42%. Это привело к ежегодной экономии бюджета в размере около 1,48 млрд. вон.

Рис. 17: Эффект от внедрения SaaS/PaaS государственными учреждениями



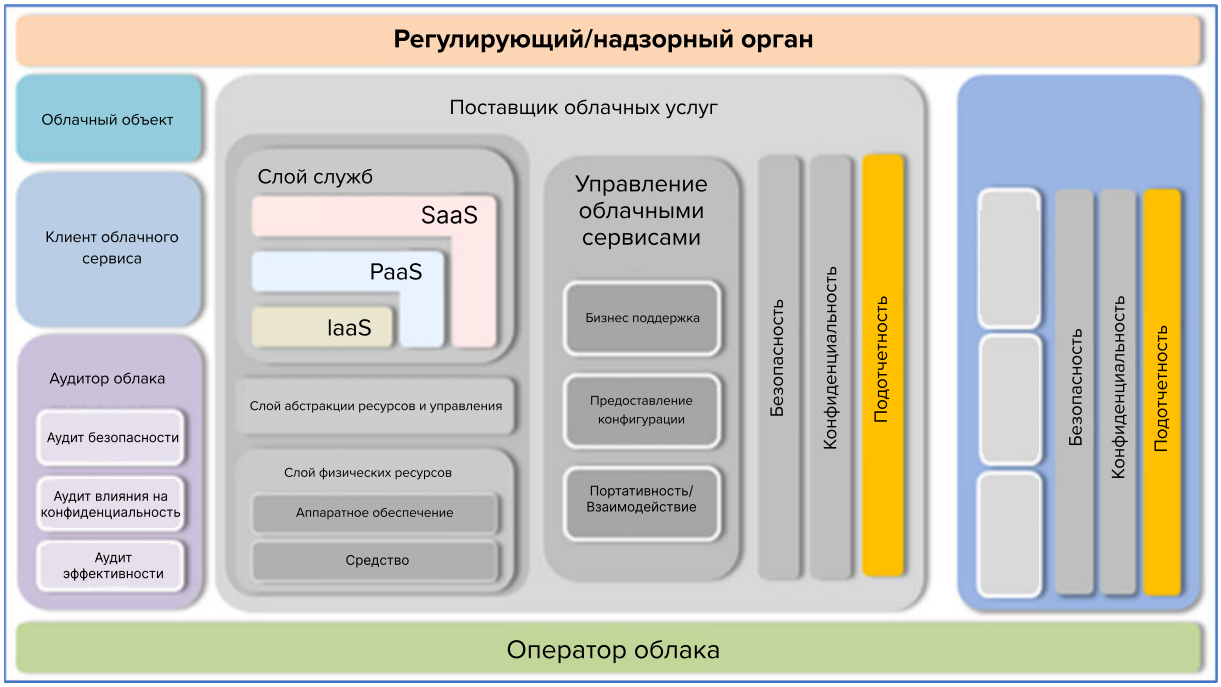


IV.9. Сравнение с другими облачными платформами

IV.9.1 Облачная платформа НИСТ

НИСТ представил комплексную эталонную облачную архитектуру, которая включает в себя сервисы и функциональные возможности заинтересованных сторон в облаке. Эта эталонная архитектура включает в себя функции потребителей облачных услуг, аудиторов, поставщиков услуг и облачных брокеров. НИСТ CCRS (Эталонная архитектура облачных вычислений) представляет концепцию абстракции ресурсов и уровня управления между уровнем обслуживания и физическим уровнем, предполагая, что сервисы должны использовать абстрактные ресурсы, а не напрямую обращаться к физическим ресурсам. Управление облачными сервисами включает в себя такие функции, как управление поддержкой бизнеса, управление предоставлением/конфигурацией и управление переносимостью/взаимодействием. Поставщики облачных услуг должны обеспечивать общие функции, такие как безопасность, конфиденциальность и подотчетность. Облачные брокеры выполняют такие задачи, как посредничество сервисов, интеграция сервисов и управление ими, для чего им требуются определенные функции. Аудиторы облака проводят такие мероприятия, как аудит безопасности, оценку влияния на конфиденциальность и аудит производительности.

Рис. 18. Эталонная архитектура облачных вычислений НИСТ.



IV.9.2 Эталонная облачная архитектура ISO/IEC 17789

В стандарте ISO/IEC 17789 CCRA (Эталонная архитектура облачных вычислений) четыре уровня определены с точки зрения пользователей облака. Его цель состоит в предоставлении стандартов для общих функций, используемых на этих уровнях.

Четыре уровня с точки зрения пользователей облака:

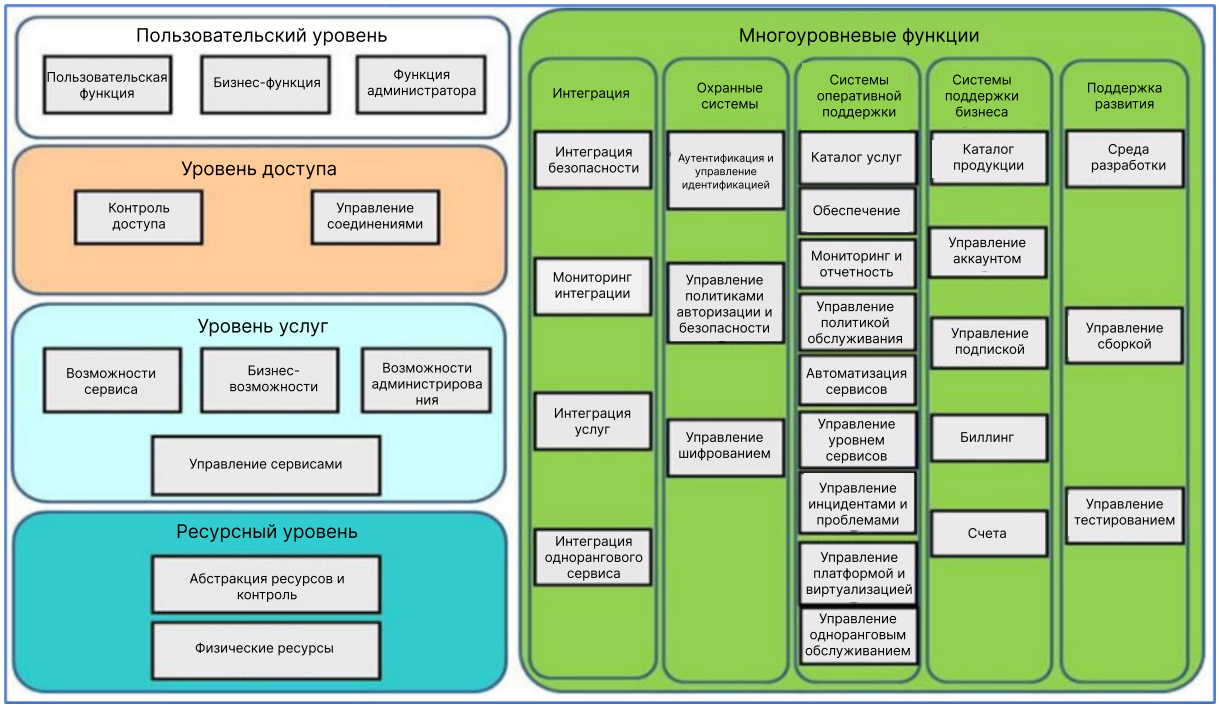
- ***Пользовательский уровень:*** функциональные компоненты, которые поддерживают деятельность облачных вычислений клиентов облачных услуг и партнеров облачных услуг.
- ***Уровень доступа:*** включает функциональные компоненты, которые облегчают развертывание и взаимодействие функций.
- ***Уровень обслуживания:*** включает функциональные компоненты, которые предоставляют сам облачный сервис, а также связанные с ним функции управления и бизнеса. Этот уровень также включает в себя функции управления, необходимые для его реализации.
- ***Уровень ресурсов:*** содержит функциональные компоненты, представляющие ресурсы, необходимые для реализации системы облачных вычислений.

Нет необходимости создавать экземпляры всех уровней или функциональных компонентов в конкретной системе облачных вычислений. Многоуровневые функциональные возможности включают функциональные компоненты, которые предоставляют функции, используемые на нескольких функциональных уровнях. Сюда входит:

- ***Поддержка разработки:*** среды разработки, поддержка сборки, управление тестированием.
- ***Интеграция:*** интеграция безопасности, интеграция мониторинга, интеграция сервисов, интеграция одноранговых сервисов.
- ***Системы безопасности:*** управление аутентификацией и идентификацией, управление авторизацией, управление политикой безопасности, управление шифрованием.
- ***Системы поддержки операций:*** каталог услуг, предоставление услуг, мониторинг и отчетность, автоматизация услуг, управление уровнем услуг, управление инцидентами и проблемами, управление платформой и виртуализацией, управление одноранговыми услугами.
- ***Системы поддержки бизнеса:*** каталог продукции, управление учетными записями, управление подписками, выставление счетов, сверка счетов.

Рис. 19. Эталонная архитектура облачных вычислений в стандарте ISO/IEC 17789.

Рис. 19. Эталонная архитектура облачных вычислений в стандарте ISO/IEC 17789.



IV.9.3 Сравнение с другими архитектурами: преимущества и ожидаемые эффекты

Облачные архитектуры НИСТ или ISO направлены на то, чтобы охватить контент, связанный с облачными вычислениями в целом, в результате чего архитектуры сосредоточены вокруг всех заинтересованных сторон облака, участвующих в предоставлении и использовании услуг. Преимущество этой перспективы заключается в расширении области применения архитектуры, что делает ее обширным стандартом, на который можно широко ссылаться. Однако когда государственным учреждениям необходимо рассмотреть архитектуру более конкретно или с технической точки зрения, это может оказаться непростой задачей.

Более того, поскольку эталонные облачные модели НИСТ или ISO в первую очередь ориентированы на IaaS (инфраструктура как услуга), государственные учреждения могут склоняться к внедрению IaaS при внедрении облачных вычислений. Однако нынешние формы внедрения облачных технологий становятся все более диверсифицированными, и все чаще рекомендуется внедрение услуг SaaS. Например, в Корее государственные учреждения активно продвигают внедрение облачных технологий, уделяя особое внимание SaaS, посредством системы специальных контрактов на цифровые услуги. Поэтому эталонная архитектура должна соответствовать этим текущим тенденциям.

Представленная нами архитектура предлагает следующие преимущества по сравнению с существующими эталонными облачными архитектурами:

- Она отражает последние тенденции облачной архитектуры. Облачные вычисления быстро развиваются от виртуальных машин к контейнерам, при этом особое внимание уделяется облачной архитектуре. Кроме того, растет популярность различных форм внедрения облачных технологий, таких как гибридное облако и мультиоблако. Цель этого документа — предоставить архитектуру, на которую можно будет опираться при внедрении таких форм облака.

- В ней представлены функциональные элементы, необходимые для конфигурации архитектуры, основанной на IaaS, PaaS и SaaS, что позволяет организациям проверять все элементы в качестве критериев при внедрении облачных вычислений. Более того, она становится техническим руководством, когда учреждения хотят выбрать один из IaaS, PaaS или SaaS при внедрении облачных вычислений.
- Число заинтересованных сторон в облаке продолжает расти, и постоянно появляется широкий спектр бизнес-форм. Таким образом, архитектура, ориентированная на определенные заинтересованные стороны, может быстро устареть. Архитектура, представленная в этом документе, исключает подход, ориентированный на заинтересованные стороны.
- В ней подробно рассматриваются функциональные элементы, которые необходимо учитывать при внедрении гибридных или мультиоблачных сервисов.
- Безопасность является решающим аспектом, когда государственные учреждения внедряют облачные вычисления, чему уделяется особое внимание на национальном уровне. Например, в США существует FedRAMP, а в Корее — CSAP. Эти системы сертифицируют структуры облачной безопасности, прежде чем государственные учреждения смогут внедрить облачные вычисления. Эти сертификаты имеют разные критерии оценки для каждого типа облака (IaaS, PaaS, SaaS). Поэтому необходимо представить структуры безопасности для каждого типа эталонной архитектуры.

IV.10. Список литературы

- ITU-T Y.3502, ‘Information technology - Cloud computing – Reference architecture’, 2014. 8.
- ISO/IEC 17789:2014 Information technology — Cloud computing — Reference architecture
- Amazon Web Services (AWS) Architecture: https://aws.amazon.com/architecture/
- Microsoft Azure Architecture: https://docs.microsoft.com/en-us/azure/architecture/
- Google Cloud Architecture: https://cloud.google.com/architecture
- OpenStack Documentation: https://docs.openstack.org/
- НИСТ Cloud Computing Publications: https://www.nist.gov/cloud-computing
- Cloud Security Alliance (CSA): https://cloudsecurityalliance.org/

I. Общий регламент защиты персональных данных (GDPR) в государственном управлении

V.1. Введение

Общий регламент защиты персональных данных (далее – GDPR), вступивший в силу 25 мая 2018 года, представляет собой важную веху в области защиты данных и конфиденциальности. Для понимания сути GDPR необходимо углубиться в его исторический контекст и основные факторы, которые привели к его принятию.

Корни GDPR уходят в середину 20-го века, когда цифровая среда была совсем другой по сравнению с сегодняшним днем. В течение этого периода начали формироваться фундаментальные принципы защиты данных в ответ на растущую обеспокоенность по поводу неприкосновенности частной жизни и безопасности данных. Это было время, когда личная информация в основном хранилась на бумажных носителях, а концепция трансграничного обмена данными еще находилась в зачаточном состоянии.

По мере того, как мир стремительно вступал в цифровую эпоху, данные становились жизненно важным ресурсом для промышленности, правительств и обществ. Благодаря Интернету данные могут распространяться по всему земному шару за считанные секунды, что открывает беспрецедентные возможности для инноваций и коммуникации, но также увеличивает риски утечки данных и нарушения конфиденциальности. Эти события побудили Европейский союз приступить к модернизации устаревших законов о защите данных.

Предшественником GDPR была Директива о защите данных 1995 года, которая определяла основополагающие принципы защиты данных в Европе. Однако, директива была признана недостаточной в условиях меняющихся цифровых сред и трансграничных потоков данных. Директива не содержала необходимые инструменты для эффективного регулирования и обеспечения защиты данных.

Потребность в более надежной и комплексной системе становилась все более очевидной по мере того, как в прессе широко освещались проблемы утечки данных, киберпреступности и нарушений конфиденциальности. Европейский союз признал, что для защиты прав и свобод своих граждан необходим более строгий и согласованный подход. Это признание положило начало разработке GDPR.

GDPR был разработан не только для укрепления прав физических лиц в отношении их персональных данных, но и для создания единой правовой базы по всему Европейскому союзу. Его создание было результатом совместных усилий с участием законодателей, экспертов по вопросам конфиденциальности и заинтересованных сторон из различных секторов. Общий регламент был разработан с целью предоставить физическим лицам больший контроль над своими персональными данными, обязать организации быть более прозрачными в отношении обработки данных и наложить значительные штрафы за несоблюдение требований.

Концепция GDPR является одним из фундаментальных ответов на меняющуюся ситуацию в области данных, подчеркивает важность защиты прав на неприкосновенность частной жизни и одновременно обеспечивает ответственное использование данных. Заложенные в нем принципы согласия, переносимости данных, права на забвение и строгие меры безопасности имеют далеко идущие последствия не только для европейцев, но и для организаций по всему миру, которые обрабатывают информацию о субъектах данных из Европы.

V.2. Важность GDPR в государственном управлении

GDPR имеет важное значение в сфере государственного управления, поскольку регламент изменяет способ, которым правительства собирают, обрабатывают и защищают персональные данные граждан. Чтобы полностью понять глубокие последствия GDPR в этом конкретном контексте, важно разобраться в том, как он влияет на государственное управление по целому ряду аспектов.

- ***Расширение прав и возможностей граждан:*** GDPR, как ответ на растущую управляемую данными среду, уделяет большое внимание правам личности. В сфере государственного управления это означает, что граждане имеют больший контроль над своими персональными данными. Правительства теперь обязаны запрашивать прямое согласие при сборе данных, быть прозрачными относительно того, как данные будут использоваться, и предоставлять гражданам простые механизмы доступа к своим данным. Это расширяет возможности граждан, предоставляя им больший контроль над информацией, хранящейся в государственных учреждениях.
- ***Повышение прозрачности:*** государственное управление часто ассоциируется с бюрократией и непрозрачностью. GDPR меняет это представление, обязывая правительства быть прозрачными в отношении своей деятельности по обработке данных. Это означает, что граждане имеют право знать, почему собираются их данные, как они будут использоваться и кто будет иметь к ним доступ. Государственные учреждения обязаны отчётливо информировать об этих процессах, укрепляя чувство доверия и подотчетности между правительством и его гражданами.
- ***Безопасность данных и подотчетность:*** в сфере государственного управления GDPR усиливает чувство ответственности. Государственные учреждения теперь придерживаются более строгих стандартов, когда дело касается безопасности данных. ГУ должны внедрять надежные меры безопасности для защиты данных граждан от взломов и несанкционированного доступа. «Статус кво» меняется с пассивного на бдительный, где защита данных становится вопросом первостепенной важности для государственных чиновников.
- ***Штрафы за несоответствие требованиям:*** GDPR предусматривает значительные штрафы за несоблюдение требований. В контексте государственного управления это правовое изменение оказывает глубокое воздействие. Это означает, что государственные учреждения сталкиваются с реальными последствиями за неправильное обращение с персональными данными. Это побуждает государственные учреждения серьезно относиться к защите данных, а также демонстрирует гражданам, что их конфиденциальность имеет огромное значение.

- ***Трансграничные потоки данных:*** государственное управление часто включает международное сотрудничество и обмен данными. Действие GDPR распространяется за пределы национальных границ, создавая гармонизированную (унифицированную) систему защиты данных по всему Европейскому союзу. Для органов государственного управления это означает оптимизированный процесс при работе с данными из нескольких государств - членов ЕС, упрощающий процедуры трансграничных потоков данных.
- ***Инновации и соответствие требованиям:*** сфера применения и цель GDPR в сфере государственного управления — это не только соблюдение требований, но и стимулирование инноваций. GDPR, требуя внедрения защиты данных в системы с самого начала, поощряет государственные учреждения творчески подходить к тому, как они могут выполнять свои обязанности, соблюдая при этом принципы конфиденциальности. Этот сдвиг в политике способствует разработке технологий и практик, повышающих конфиденциальность.

В целом, GDPR трансформирует государственное управление, ставя во главу угла защиту данных и конфиденциальность граждан. GDPR расширяет права и возможности граждан, повышает прозрачность, обеспечивает безопасность данных и прививает чувство подотчетности. Органы государственного управления больше не являются простыми хранителями данных, а теперь являются хранителями доверия граждан и прав на данные, способствуя более ответственному и ориентированному на граждан подходу к управлению в эпоху цифровых технологий.

V.3. Обзор GDPR и его основных положений

GDPR стал механизмом защиты, который меняет способы обработки персональных данных организациями. Его основные положения, которые мы более подробно рассмотрим ниже, подчеркивают основные принципы и правила, которые определяют этот важный регламент. Сюда входят:

- ***Территориальная сфера действия:*** представьте себе регулирование, не знающее границ. Территориальная сфера действия GDPR является отличительной чертой, распространяющей его действие не только на организации в Европейском союзе, но и за его пределами, при условии, что они обрабатывают персональные данные резидентов ЕС. Экстерриториальное применение означает, что компании по всему миру должны соблюдать его принципы при обработке данных граждан ЕС.
- ***Согласие:*** представьте себе потенциального клиента, просматривающего веб-сайт. Клиента просят принять файлы cookie, процесс становится понятным и простым. В основе GDPR лежит принцип ясного и недвусмысленного согласия. Регламент настоятельно требует, чтобы организации запрашивали такое согласие у субъектов данных, прежде чем обрабатывать их данные. Согласие должно быть добровольным, конкретным, информативным и легко отзываемым. GDPR передает полномочия по контролю за данными в руки самих граждан.
- ***Права субъекта данных:*** представьте, что у вас есть ключ к собственному царству данных. В соответствии с GDPR физическим лицам был предоставлен ряд прав, связанных с их персональными данными. Во-первых, право на доступ к своим данным похоже на то, чтобы повернуть ключ и получить доступ к сокровищнице

информации о том, что организации хранят о них. Право исправлять неточные данные равносильно тому, чтобы иметь возможность исправить собственную историю. Кроме того, существует право на удаление данных, которое часто называют «правом на забвение». Это дает физическим лицам право требовать удаления своих данных при определенных обстоятельствах. Наконец, право на переносимость данных подобно тому, как человеку выдаются ключи, позволяющие разблокировать свои данные и взять их с собой, беспрепятственно перемещаясь по различным сервисам.

- ***Сотрудники по защите данных (англ. DPOs):*** представьте себе, что вы управляете огромной организацией, осуществляющей масштабные операции с данными. Нужен кто-то, кто проведет вас через лабиринт данных. Это роль сотрудника по защите данных. Согласно GDPR требуется чтобы определенные организации, особенно те, которые обрабатывают значительные объемы конфиденциальных данных, назначали сотрудника по защите данных. Какова миссия сотрудника по защите данных? Обеспечить соблюдение организацией требований GDPR и защищать права субъектов данных на неприкосновенность частной жизни.
- ***Уведомление об нарушении безопасности персональных данных:*** в мире, где нарушения безопасности персональных данных представляет собой надвигающуюся угрозу, в рамках GDPR вводится важная концепция — своевременное уведомление. Организации должны сообщать о нарушениях соответствующим госорганам и пострадавшим лицам в течение 72 часов с момента получения информации о нарушении. Данное уведомление содержит важную информацию о характере нарушения и его потенциальных последствиях. Это похоже на систему быстрой сигнализации, обеспечивающую обнаружение нарушений с целью предотвращения их сокрытия в течение длительного времени.
- ***Оценки воздействия на защиту данных (англ. DPIAs):*** представьте себе тщательную оценку рисков перед путешествием. GDPR предписывает проводить оценку воздействия на защиту данных для операций по обработке данных, которые представляют высокий риск для конфиденциальности физических лиц. Эти оценки похожи на выявление потенциальных подводных камней перед путешествием, они помогают организациям выявлять и минимизировать риски конфиденциальности, и тем самым приводят обработку данных в соответствие с принципами GDPR.
- ***Конфиденциальность по замыслу и по умолчанию:*** подумайте о строительстве дома с учетом безопасности с самого начала. В этом суть «конфиденциальности по замыслу» и «конфиденциальности по умолчанию» в соответствии с GDPR. Конфиденциальность по замыслу побуждает организации с самого начала интегрировать защиту данных в разработку систем и сервисов. Конфиденциальность по умолчанию требует, чтобы автоматически применялись самые строгие настройки конфиденциальности. Это означает, что основополагающая структура обработки данных по своей сути безопасна и обеспечивает соблюдение конфиденциальности.
- ***Передача данных:*** представьте себе данные как ценный, хрупкий груз, перевозимый через границы. GDPR устанавливает правила передачи персональных данных за пределы ЕС, гарантируя, что такая передача соответствует стандартам GDPR и защищена соответствующими мерами безопасности. По аналогии с обеспечением сохранности ценного груза во время перевозки, независимо от пункта назначения.

- ***Учёт и управление:*** учет и управление подобны своду правил и арбитру в области защиты данных. GDPR подчеркивает, что организации должны вести подробный учет деятельности по обработке данных, проводить регулярные аудиты и внедрять соответствующие политики и меры по защите данных. Это способствует формированию культуры ответственности и прозрачности, гарантируя, что все играют по правилам.
- ***Штрафы:*** считайте штрафы, предусмотренные GDPR, мечом правосудия в области защиты данных. Одним из наиболее примечательных аспектов GDPR являются значительные штрафы, которые предусмотрены за несоблюдение. За серьезные нарушения организации могут быть оштрафованы на сумму до 4% от их совокупного (мирового) годового дохода или 20 миллионов евро, в зависимости от того, что больше. Этот финансовый риск является существенным стимулом для организаций к тому, чтобы уделять приоритетное внимание соблюдению требований GDPR.

Подводя итоги, можно сказать, что в мире, где персональные данные являются ценным товаром и потенциальным источником вреда, GDPR выступает в качестве ключевого механизма защиты. Его основные положения позволяют физическим лицам контролировать свои данные и устанавливают строгие правила, которым должны следовать организации. Соблюдение требований GDPR необходимо для создания более безопасной, ответственной и ориентированной на конфиденциальность цифровой среды, где защита данных является не просто нормативным актом, а фундаментальным правом.

V.4. Историческое развитие законодательства в области защиты данных

Историческое развитие законодательства в области защите данных, в конечном итоге привело к Общему регламенту защиты персональных данных (далее – GDPR), представляет собой путешествие во времени, свидетельствующее о растущем признании важности защиты персональной информации. История начинается с осознания того, что персональные данные не только ценны, но и уязвимы. В начале 1970-х годов Швеция стала первой в мире страной, принявшей закон о защите данных. Движение за защиту данных, укоренившись, распространилось по всей Европе и другим частям света.

Поворотный момент относительно конфиденциальности данных приходится примерно на 1981 год, когда цифровая революция начала ускоряться, и возросли опасения по поводу обработки персональных данных. Фактически, Совет Европы принял Конвенцию о защите физических лиц в отношении автоматической обработки персональных данных в 1981 году; он стал знаковым международным договором. Он ознаменовал первую международную попытку решения вопросов защиты данных и конфиденциальности. Данный процесс продолжился в 1995 году с принятием Директивы Европейского союза о защите данных. Эта директива заложила основу для законов о защите данных во всех государствах - членах ЕС, подчеркнув необходимость защиты персональных данных и изложив принципы их законной обработки. Эти принципы легли в основу последующих разработок в области защиты данных.

С экспоненциальным ростом Интернета и цифровых технологий стала очевидной необходимость в более надежных мерах защиты данных. По мере того, как потоки

данных стали выходить за рамки границ и появлялись новые формы обработки данных, росли опасения по поводу недостаточности существующих нормативных актов. В 21-м веке законы о защите данных требовали существенного обновления с учетом меняющейся ситуации с конфиденциальностью данных. Результатом этой работы стал Общий регламент защиты персональных данных (GDPR), который вступил в силу в мае 2018 года. GDPR стал поворотным моментом в истории защиты данных. В нем сочетались принципы и концепции более ранних нормативных актов с современным пониманием эпохи цифровых технологий. GDPR направлен на гармонизацию законодательства в области защите данных по всему ЕС и предоставление физическим лицам большего контроля над своими персональными данными.

Несомненно, GDPR принес много преимуществ, но вместе с тем, он привел к ряду проблем. Регламент расширил права на неприкосновенность частной жизни, укрепил безопасность данных и способствовал укреплению общественного доверия к цифровому миру, который часто страдает от нарушения безопасности данных. Однако GDPR также создает серьезные проблемы для организаций по всему миру, особенно для тех, которые не привыкли к таким строгим требованиям к защите данных. Усилия по обеспечению соответствия требуют существенных инвестиций в технологии и изменений в корпоративной культуре. Также очевидно, что влияние GDPR распространяется за пределы Европейского союза. Экстратерриториальный принцип регламента влияет на организации по всему миру, вынуждая их адаптироваться к его принципам, если они обрабатывают персональные данные резидентов ЕС. Глобальное воздействие подчеркивает значимость GDPR и его актуальность в глобальном масштабе.

Идеологическая концепция законодательства в области защиты данных, результатом которой стал GDPR, — это история растущей осведомленности и реагирования на вызовы, возникающие в эпоху цифровых технологий. GDPR подчеркивает растущее признание ценности персональных данных и необходимости их защиты. GDPR представляет собой результаты этих усилий, предлагая комплексную основу для защиты персональной информации во все более взаимосвязанном и управляемом данными мире. Эта путь, охватывающий несколько десятилетий, показывает, что защита данных превратилась из узкоспециализированной проблемы в глобальный императив, устанавливающий стандарт ответственного обращения с данными и конфиденциальности личности в современную эпоху.

V.5. Основные принципы GDPR

GDPR основан на нескольких основных принципах, которые определяют обработку персональных данных:

- ***Законность, справедливость и прозрачность:*** в соответствии с требованиями GDPR персональные данные должны обрабатываться законно, справедливо и прозрачно. Это означает, что организации должны иметь законные основания для обработки данных, такие как согласие, договорные обязательства или законный интерес. Кроме того, организации должны быть прозрачны в отношении того, как используются данные, предоставляя физическим лицам четкую и понятную информацию о деятельности по обработке данных. Прозрачность имеет решающее значение для укрепления доверия между физическими лицами и организациями.

- ***Ограничение целью:*** персональные данные должны собираться для конкретных, отчетливых и законных целей и не подлежат дальнейшей обработке несовместимым с этими целями образом. Этот принцип не позволяет организациям использовать данные в целях, не связанных с первоначальным намерением сбора, гарантируя, что данные физических лиц не будут подвержены неправомерному использованию.
- ***Минимизация данных:*** в GDPR подчеркивается, что организации должны собирать только те данные, которые необходимы для указанных целей. Минимизация данных снижает риск нарушения безопасности данных и защищает конфиденциальность физических лиц, ограничивая объем собираемых данных до самого необходимого.
- ***Точность:*** организации несут ответственность за обеспечение точности персональных данных. Данные необходимо поддерживать в актуальном состоянии и исправлять при выявлении неточностей. Неточные данные могут привести к неправильным решениям, наносящим ущерб интересам физических лиц.
- ***Ограничение хранения:*** персональные данные не должны храниться дольше, чем необходимо для тех целей, в связи с которыми они собирались. Организации должны установить политику хранения и удалять данные, когда они больше не нужны, снижая риск, связанный с хранением избыточных данных.
- ***Целостность и конфиденциальность:*** этот принцип требует от организаций принятия мер безопасности для защиты персональных данных от несанкционированного доступа, раскрытия, изменения или уничтожения. Для обеспечения целостности и конфиденциальности данных необходимы шифрование, контроль доступа и регулярные оценки безопасности.
- ***Учёт и управление:*** в соответствии с требованиями GDPR организации должны нести ответственность за свою деятельность по обработке данных. Организации должны внедрять политики, процедуры и другие документы, подтверждающие соответствие регламенту. Оценки воздействия на защиту данных и сотрудники по защите данных играют решающую роль в обеспечении подотчетности.
- ***Права субъекта данных:*** GDPR наделяет субъектов персональных данных несколькими правами в отношении их данных. Эти права включают, среди прочего, право на доступ к своим данным, исправление неточностей, запрос на удаление (право на забвение) и возражение против обработки данных. Организации обязаны содействовать осуществлению этих прав, предоставляя физ. лицам контроль над их личной информацией.

В целом, основные принципы GDPR в совокупности создают прочную основу для защиты данных и конфиденциальности в эпоху цифровых технологий. Эти принципы гарантируют, что персональные данные обрабатываются законно, справедливо и прозрачно, с ясными целями и минимальным сбором данных. Вместе с тем, они подчеркивают важность точности данных, безопасного хранения и подотчетности. Права, предоставляемые субъектам данных, позволяют физическим лицам контролировать свою персональную информацию, усиливая важность соблюдения конфиденциальности и защиты данных во все более взаимосвязанном мире.

V.6. Сертификация

В соответствии со статьей 42 GDPR нормативно-правовая база позволяет органу по защите данных каждой страны создавать свою собственную систему сертификации.

Однако создание общеевропейского механизма сертификации требует одобрения Европейского совета по защите данных (англ. EDPB). В мае 2022 года Национальная комиссия по защите данных (англ. CNPD) приняла механизм сертификации GDPR-CARPA, что ознаменовало значительный шаг вперед. Позже в том же году, в октябре, Европейский совет по защите данных одобрил механизм сертификации Euro privacy в качестве европейского знака защиты данных в соответствии со статьей 42(5). Эти два механизма сертификации обладают уникальными характеристиками и критериями, способствующими соблюдению требований GDPR и защите данных в Европе. Давайте углубимся в специфику GDPR-CARPA и Euro privacy, чтобы получить более глубокое представление об их целях, сферах применения и последствиях. В соответствии со статьей 42 орган по защите данных каждой страны может создать собственную систему сертификации, а механизм сертификации в масштабах всего Европейского Союза требует одобрения Европейского совета по защите данных. В мае 2022 года Национальная комиссия Люксембурга по защите данных приняла механизм сертификации GDPR-CARPA. Позже в том же году, в октябре, Европейский совет по защите данных одобрил механизм сертификации Euro privacy в качестве европейского знака защиты данных в соответствии со статьей 42(5).

V.6.1 GDPR-CARPA

GDPR-CARP - это первый механизм сертификации, разработанный и принятый Национальной комиссией по защите данных на национальном и международном уровне в соответствии с GDPR в мае 2022 года. Этот механизм имеет несколько ключевых особенностей, включая его цель, поддержание и область применения, что является критическим для понимания его роли в обеспечении соответствия требованиям GDPR и защиты данных.

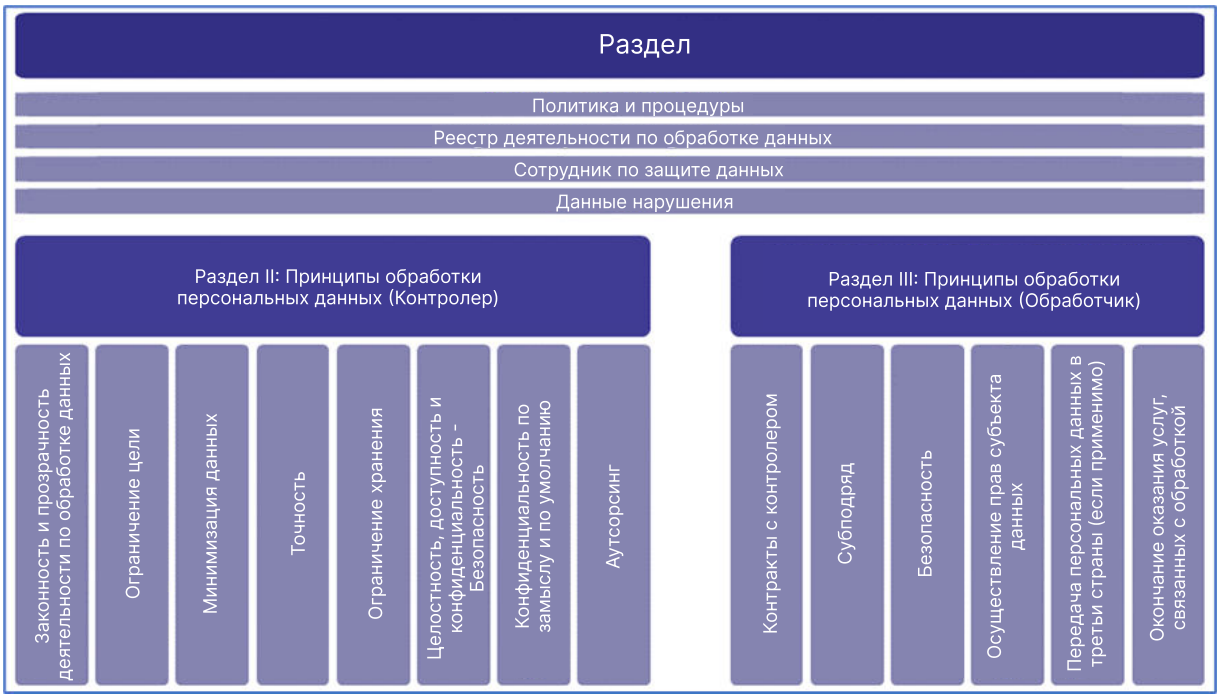
- ***Цель:*** сертификация предназначена для того, чтобы обеспечить контролерам и обработчикам данных высокий уровень соответствия GDPR и гарантировать, что они применяют технические и организационные меры для соблюдения своих обязательств в рамках GDPR.
- ***Поддерживается*** Национальной комиссией по защите данных Люксембурга (Commission nationale pour la protection des données, CNPD).
- ***Требование заявляющей стороны:*** запрос на сертификацию GDPR-CARPA может подать только контролер или обработчик, зарегистрированный в Люксембурге под надзором Национальной комиссии по защите данных.
- ***Область сертификации:*** механизм сертификации не удостоверяет всю организацию, а конкретные операции по обработке данных.
- ***Ограничение юридической силы:*** сертификация показывает соблюдение требований GDPR, но не снижает ответственность контролера или обработчика. Механизм сертификации GDPR-CARPA фокусируется на системе управления для определения и внедрения мер по информационной безопасности в пределах ее сферы применения. По сути, сертификация показывает соответствие требованиям GDPR посредством надлежащей практики управления.
- ***Срок действия***: сертификат действителен в течение 3 лет и может быть продлен при условии проведения ежегодной аудиторской проверки.
- ***Критерии оценки:*** критерии сертификации GDPR-CARPA разделены на три раздела.

Раздел 1 Общее руководство по защите данных, включая политики и процедуры, учет деятельности по обработке данных, права субъектов данных, сотрудник по защите данных, нарушения данных.

Раздел 2 Обязательства контролеров в отношении принципов защиты данных в соответствии со статьей 5.

Раздел 3 Обязательства обработчиков, такие как заключение контрактов с контролерами и субподрядчиками, обеспечение безопасности, передача персональных данных в третьи страны.

Рис. 20: Критерии подотчетности



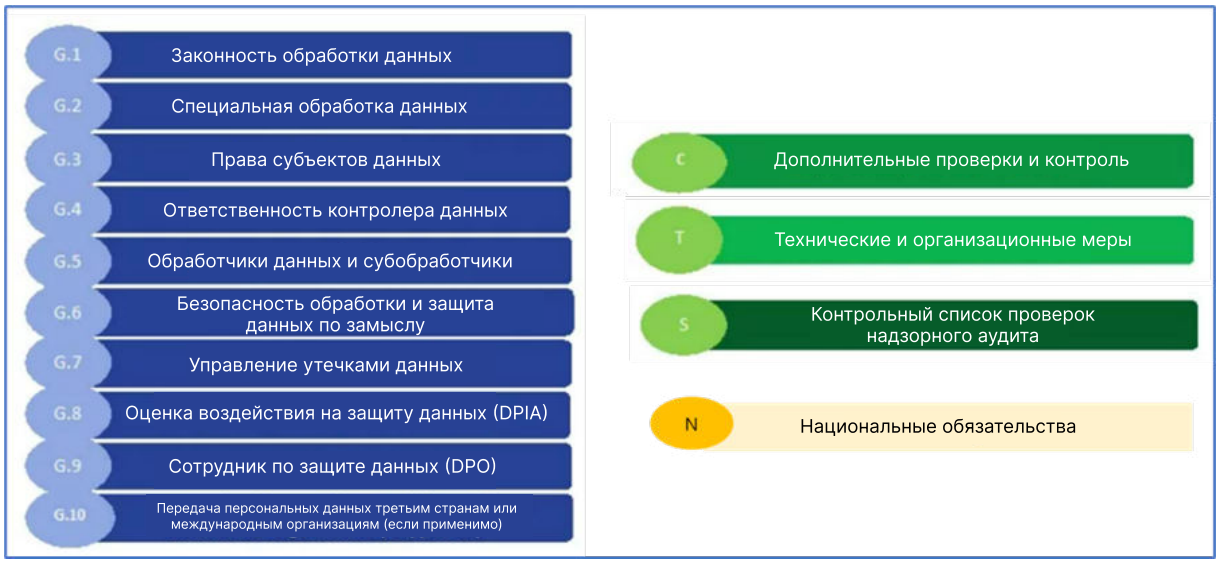
V.6.2 Euro privacy

Euro Privacy принимается в качестве европейского знака защиты данных (статья 42(5)) в 2022 году и в настоящее время является единственным механизмом сертификации, признанным во всех странах-членах Европейского союза. Его значимость подчеркивается несколькими ключевыми атрибутами, включая его цель, поддержание и область применения, что является критическим для понимания его роли в демонстрации соответствия требованиям GDPR и защиты данных в общеевропейском масштабе.

- ***Цель*** - демонстрация соблюдения требований GDPR при операциях по обработке данных контролерами и обработчиками.
- ***Поддерживается*** Европейским центром сертификации (англ. ECCP).
- ***Требование заявляющей стороны*** – неприменимо.
- ***Область сертификаци***и - сертификация распространяется на деятельность по обработке данных (вся компания или ее система управления в целом не могут быть сертифицированы).
- ***Ограничение юридической силы*** - сертификация не снижает ответственность контролера или обработчика за соблюдение требований GDPR и не затрагивает задачи и полномочия надзорных органов, компетентных в соответствии со статьями 55 или 56 (статья 42(4)).

- ***Срок действия*** – 3 года.
- ***Критерии оценки*** – критерии оценки Euro Privacy легко интегрируются с ISO/IEC 27001 и делятся на две части: основные критерии, охватывающие различные обязательства по GDPR, и дополнительные критерии, обозначенные как C, T, S, N.
- ***Основные критерии*** – законность обработки данных, обработка специальных категорий данных, права субъектов данных, ответственность контролеров данных, обработчиков данных (или субобработчиков), безопасность обработки и защита данных по замыслу, управление происшествиями, связанными с безопасность данных, оценка воздействия на защиту данных (англ. DPIA), сотрудник по защите данных (англ. DPO), передача персональных данных третьим странам или международным организациям.
- ***Дополнительные проверки и контроль (C)*** - оценка соответствия обязательствам, относящимся к конкретной предметной области и технологии.

Рис. 21: Основные критерии GDPR

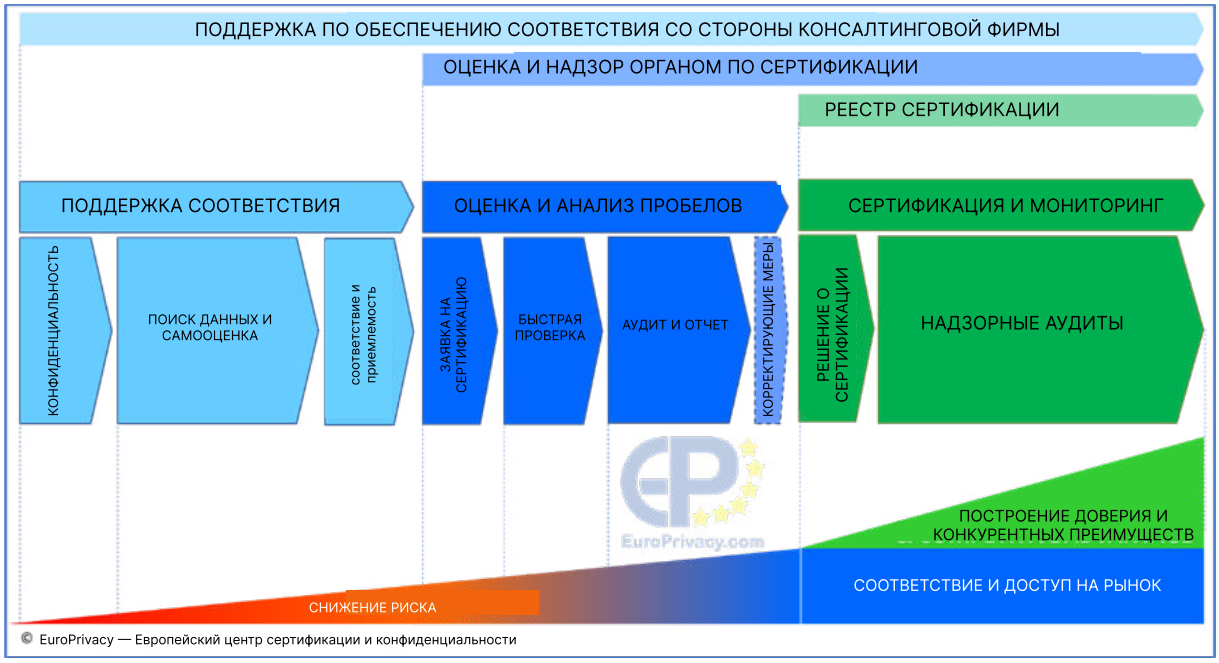


- ***Технические и организационные меры (T)*** - оценка достаточности принятых мер по обеспечению безопасности обрабатываемых данных. В случае обработки данных с высоким риском, то их можно заменить действующим сертификатом ISO/IEC 27001.
- ***Контрольный список надзорных аудитов (S)*** – оценка и обеспечение постоянного соблюдения требований с течением времени.
- ***Национальные обязательства (N)*** - оценка дополнительных национальных обязательств с помощью профилей национальных обязательств для каждого из государств - членов Европейской экономической зоны, а также необязательная и расширенная оценка юрисдикций, не входящих в ЕС.

V.6.3. Процесс сертификации

Европейский центр сертификации предоставляет различные онлайн-ресурсы, и его рекомендации могут быть полезными при внедрении GDPR или подготовки к сертификации Euro Privacy.

Рис. 22: Процесс сертификации



V.7. Влияние GDPR на государственное управление

GDPR служит маяком для защиты прав и конфиденциальности данных в цифровую эпоху. Поскольку данный Регламент распространяется на различные отрасли, его влияние на государственного управление заслуживают особого внимания. Государственные организации, которым доверены огромные объемы персональных данных, играют важнейшую роль в обеспечении соблюдения принципов GDPR. В данном разделе рассматривается влияние GDPR на государственное управление, проливая свет на трансформационные изменения в управлении и предоставлении государственных услуг в результате принятия GDPR.

- ***Изменения в методах сбора данных:*** с внедрением GDPR в государственном управлении произошли значительные изменения в методах сбора данных. Принцип минимизации данных означает, что можно собирать только те данные, которые необходимы для конкретной цели. Это потребовало от государственных органов переоценки и зачастую рационализации запрашиваемых у населения данных. Кроме того, принцип прозрачности предполагает необходимость четкого информирования граждан о целях сбора данных. В результате государственные ведомства были вынуждены переработать формы, приложения и онлайн-порталы, чтобы обеспечить получение прямого согласия и ясное указание цели сбора данных.
- ***Изменения в области хранения и защиты данных:*** требования GDPR по обеспечению безопасности потребовали значительных изменений в способах хранения и защиты персональных данных в государственных органах. Госорганам пришлось инвестировать в модернизацию своих систем хранения данных, чтобы обеспечить шифрование и другие меры защиты. Кроме того, требование GDPR об ограничении хранения означает, что данные больше не могут храниться бесконечно. Государственные организации должны внедрять четкие графики хранения данных и периодически пересматривать их, а также удалять данные,

которые больше не служат законным целям. Кроме того, важное значение приобрели планы действий на случай непредвиденных обстоятельств, включая надежные системы резервного копирования и протоколы реагирования на инциденты нарушения безопасности данных.

- ***Расширение прав субъектов данных:*** одним из наиболее значимых влияний GDPR на государственное управление стала необходимость признания и содействия расширению прав субъектов данных. Теперь граждане имеют право получать доступ к своим данным, исправлять неточности и даже требовать их удаления в определенных обстоятельствах (часто это называют «правом на забвение»). Государственные ведомства, от здравоохранения до жилищно-коммунального хозяйства, вынуждены создавать каналы и системы, позволяющие гражданам беспрепятственно реализовывать эти права. Это включает в себя предоставление платформ для запросов на доступ к данным, обеспечение своевременного ответа на них, а также предоставление механизмов исправления или удаления данных.
- ***Требования к подотчетности и отчетности:*** согласно GDPR, на государственные органы ложится основная нагрузка по доказательству соблюдения принципов защиты данных. Это чувство подотчетности требует всестороннего учета всех действий по обработке данных. В случае утечки данных или любого другого нарушения государственные органы обязаны строго соблюдать установленный срок (обычно 72 часа), в течение которого они должны сообщить о случившемся в соответствующий надзорный орган. Это привело к созданию во многих государственных органах специальных групп по защите данных, которые отвечают за постоянное соблюдение требований GDPR, оценку рисков и взаимодействие с органами по защите данных.
- ***Влияние на договоры и отношения с третьими сторонами:*** действие GDPR распространяется не только на государственные органы, но и на любые сторонние организации, с которыми они сотрудничают или заключают договоры на оказание услуг. Сфера действия GDPR распространяется не только на государственные органы, но и на любые сторонние организации, с которыми они сотрудничают или заключают договоры на оказание услуг. В результате государственным органам пришлось пересмотреть и перезаключить договоры, включив в них строгие положения о защите данных. Проверки на предмет соблюдения требований GDPR третьими сторонами стали нормой, а во многих случаях для обеспечения постоянного соблюдения стандартов защиты данных проводятся постоянные аудиторские проверки.

По сути, принятие GDPR ознаменовало период преобразований для государственного управления в области защиты данных. Все аспекты государственного управления, от основополагающих методов сбора данных до сложной динамики взаимоотношений с третьими сторонами, были перестроены с целью соблюдения неприкосновенности персональных данных и защиты прав граждан. Эти изменения имеют глубокие последствия, способствуя формированию более прозрачной, подотчетной и ориентированной на граждан модели управления.

V.8. Практические шаги по внедрению

Цель данного раздела - выделить важнейшие меры, которые необходимо принять государственным органам для достижения соответствия требованиям GDPR. Основное внимание уделяется выработке единой стратегии, подчеркивающей важность укрепления доверия граждан и обеспечивающей максимальную защиту целостности данных.

- ***Назначение сотрудника по защите данных (англ. DPO):*** назначение сотрудника по защите данных является одним из основных шагов по приведению регулирования в соответствие с требованиями GDPR. Сотрудник по защите данных играет ключевую роль в обеспечении соблюдения организацией правил защиты данных. Они выступают в качестве координаторов всех мероприятий по защите данных, начиная от консультаций по соблюдению требований и заканчивая представлением интересов организации в органах по защите данных. В частности, для государственных органов, работающих с большими объемами конфиденциальных данных, сотрудник по защите данных обеспечивает постоянный контроль, своевременное вмешательство и выступает в качестве связующего звена между субъектами данных и организацией.
- ***Проведение оценок воздействия на защиту данных (англ. DPIA):*** оценки воздействия на защиту данных являются важнейшими инструментами в наборе средств обеспечения соответствия требованиям GDPR. Процесс предусматривает систематическую оценку потенциальных рисков, связанных с деятельностью по обработке данных. Проведение оценок позволяет государственным органам выявить уязвимые места в процессах обработки данных и принять меры по их устранению до того, как будет нанесен ущерб. Такой проактивный подход обеспечивает решение проблем конфиденциальности с самого начала, что делает его неотъемлемой частью любого проекта или инициативы, связанного с большими объемами данных.
- ***Внедрение подхода «защита данных по замыслу и по умолчанию»:*** этот принцип требует, чтобы меры по защите данных были интегрированы уже на этапе разработки любого проекта или системы и действовали по умолчанию. Это означает, что при создании нового цифрового сервиса или инфраструктуры его основополагающие элементы должны быть ориентированы на защиту данных. Данный подход потребует от государственных органов смены парадигмы: от ретроактивных проверок соблюдения требований к проактивному включению защиты данных в принципы проектирования. Будь то новая база данных здравоохранения или портал цифровых услуг, архитектура должна обеспечивать защиту персональных данных.
- ***Обеспечение безопасной обработки и хранения данных:*** в основе GDPR лежит безопасная и законная обработка персональных данных. Государственные органы должны использовать самые современные методы шифрования для обеспечения защиты передаваемых и хранимых данных. Кроме того, для предотвращения несанкционированного доступа и возможных нарушений обязательны надежный контроль доступа, регулярное обновление систем и оценка уязвимостей. Это касается не только цифровых носителей: даже физические документы, содержащие персональные данные, должны надежно храниться, а доступ к ним строго контролироваться.

- ***Разработка и внедрение протоколов по борьбе с утечкой данных:*** несмотря на все меры предосторожности, утечка данных все равно может произойти. Государственным органам крайне важно иметь четкий и эффективный протокол реагирования. Это включает в себя немедленную локализацию нарушения, оценку его масштабов и последствий, своевременное уведомление пострадавших лиц и представление информации в надзорные органы в течение предписанных 72-часов. Наличие хорошо отработанного протокола позволяет существенно минимизировать ущерб и обеспечить быстрое восстановление после любого нарушения.
- ***Обучение и информационные кампании для персонала:*** человеческий фактор зачастую является самым слабым звеном в защите данных. В этой связи, регулярное обучение и информационно-просветительские кампании для персонала имеют решающее значение. Сотрудники всех уровней должны быть проинформированы о принципах GDPR, правах субъектов данных и протоколах, которым необходимо следовать в различных сценариях. Хорошо обученный персонал - от распознавания попыток фишинга до понимания нюансов получения согласия - является первой линией обороны организации от потенциальных нарушений защиты данных.

По сути, практическая реализация GDPR в государственных органах — это многогранная работа, требующая как технологической адаптации, так и культурных сдвигов. Каждый из этих шагов, от назначения сотрудника по защите данных (DPO) до обучения персонала, способствует созданию устойчивой, прозрачной и подотчетной экосистемы защиты данных, обеспечивая соблюдение прав граждан и их доверие к государственным органам.

V.9. Трудности при внедрении GDPR в государственном управлении

В данном разделе рассматриваются различные препятствия, с которыми сталкиваются государственные органы при выполнении требований GDPR, изучается сложная взаимосвязь между технологическими, бюрократическими и практическими проблемами.

- ***Технологические проблемы:*** внедрение GDPR в государственном управлении повлекло за собой ряд технологических проблем. Поскольку системы и инфраструктура обработки данных, используемые во многих государственных секторах, зачастую были созданы несколько лет назад, их обновление в соответствии с современными требованиями GDPR может оказаться непростой задачей. Это включает шифрование передаваемых и хранимых данных, интеграцию систем для беспрепятственного и безопасного доступа к данным, а также обеспечение устойчивости к киберугрозам. Кроме того, старые системы могут быть несовместимы с новыми протоколами безопасности, что требует комплексного пересмотра системы, а не пошаговых обновлений.
- ***Бюрократические препятствия:*** государственные органы по своей природе имеют многоуровневую бюрократию. Это может создать проблемы при попытке быстрого и эффективного внедрения положений GDPR. Например, получение необходимых разрешений на внесение изменений в систему, координация действий различных подразделений или просто следование сложному комплексу

административных процессов могут затянуть процесс согласования GDPR. Кроме того, в процессе принятия решений в государственных организациях часто участвует множество заинтересованных сторон, что может замедлить принятие критически важных мер по защите данных.

- ***Финансовые последствия:*** финансовая нагрузка, связанная с соблюдением GDPR, может быть существенной, особенно для государственных органов, которые работают с ограниченным бюджетом. Затраты, связанные с обновлением ИТ-инфраструктуры, наймом или обучением специализированного персонала, например, сотрудников по защите данных, а также проведением регулярных аудиторских проверок и оценок, могут быстро нарастать. Кроме того, потенциальные финансовые штрафы за несоблюдение требований GDPR требуют от государственных органов достаточных инвестиций в инициативы, связанные с GDPR, что создает нагрузку на и без того ограниченные ресурсы.
- ***Баланс между прозрачностью и защитой данных:*** одним из основных принципов государственного управления является прозрачность. Однако GDPR требует строгой защиты данных, и найти баланс между этими двумя требованиями может быть непросто. Несмотря на то, что у граждан есть право на доступ к информации и понимание государственных процессов, обеспечение защиты персональных данных при этом может оказаться непростой задачей. Принятие решения о том, что и в каком объеме раскрывать, а также обеспечение того, чтобы раскрытие не привело к непреднамеренной утечке персональных данных, требует тщательного планирования и исполнения.
- ***Обеспечение согласованного применения в различных государственных структурах:*** государственные органы — это не монолитные структуры, а скорее конгломерат различных подразделений, каждое из которых имеет свой комплекс задач, ресурсов и приоритетов. Обеспечение последовательного применения GDPR во всех этих структурах может представлять собой серьезную проблему. Мера, которая хорошо работает в одном подразделении, может столкнуться с сопротивлением или проблемами при ее внедрении в другом. Координация соблюдения требований GDPR в различных подразделениях, обеспечение однородных стандартов и решение уникальных проблем для каждого подразделения требуют всестороннего, хорошо организованного подхода.

Таким образом несмотря на то, что GDPR представляет собой план по защите данных и конфиденциальности, его реализация в рамках государственного управления сопряжена с определенными трудностями. Эти препятствия, начиная от технологических ограничений и заканчивая бюрократической волокитой, требуют не только ресурсов, но и тонкого понимания как GDPR, так и тонкостей государственного управления. Однако при совместных усилиях эти проблемы можно преодолеть, приведя государственное управление в соответствие с золотым стандартом защиты данных.

V.10. Примеры из практики: примеры внедрения GDPR в государственном управлении

В разных странах разработаны собственные общие принципы и стандарты, обеспечивающие защиту персональных данных и соответствие требованиям GDPR, принятом Европейским союзом. Цель этих инициатив – предоставить организациям практические рекомендации и меры по выполнению требований законодательства и повышению уровня безопасности данных.

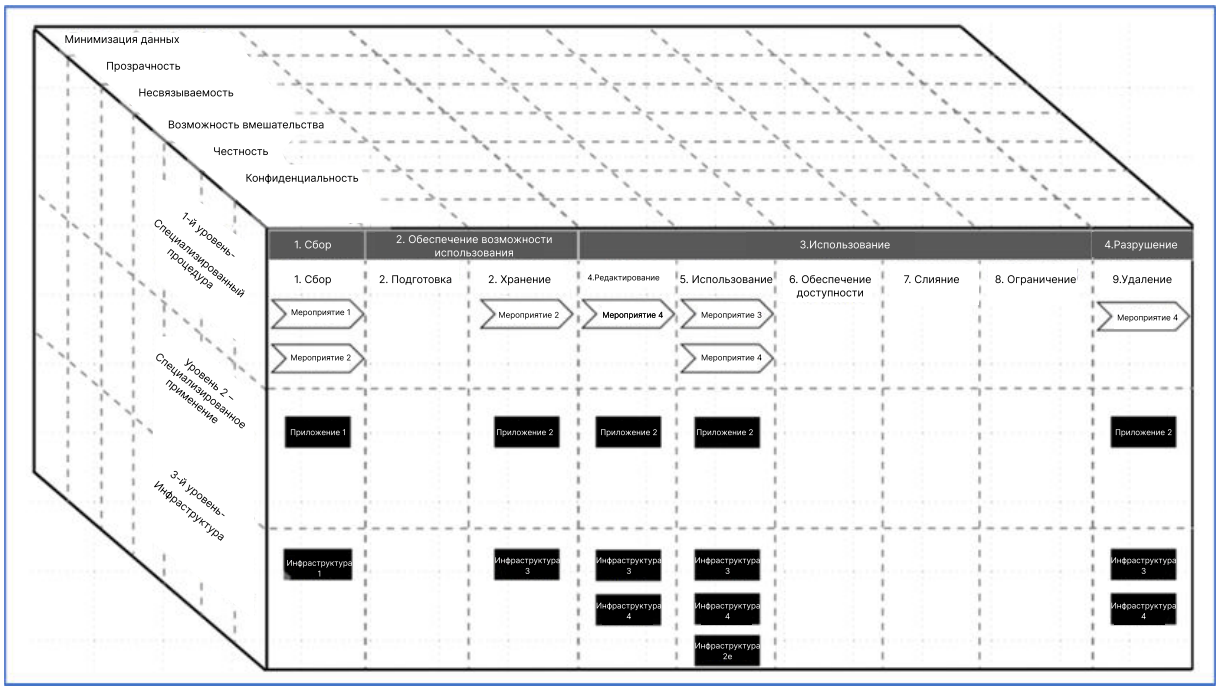
V.10.1 Германия - Стандартная модель защиты данных

Стандартная модель данных (англ. SDM), разработанная Конференцией независимых органов по защите данных Германии (Datenschutzkonferenz или DSK), служит практической базой, преобразующей юридические требования GDPR в конкретные технические и организационные мероприятия. Это упрощает переход от абстрактных юридических обязательств к конкретным, выполнимым действиям. Последняя версия (3.0) была принята в 2022 году.

Стандартная модель защиты данных (англ. SDM) применяется при планировании, реализации, эксплуатации, экспертизе и оценке деятельности по обработке персональных данных. Модель предназначена для оказания помощи организациям как коммерческого, так и государственного сектора при предоставлении документов, демонстрирующих соблюдение норм GDPR, а также установление механизмов ответственности за обработку персональных данных.

Требования законодательства выражаются в семи основных «гарантиях, которые должны быть достигнуты», включающих в себя (1) минимизацию данных, (2) доступность, (3) целостность, (4) конфиденциальность, (5) невозможность обратной идентификации, (6) прозрачность и (7) возможность вмешательства (контроль со стороны субъектов данных).

Рис. 23: Куб стандартной модели данных (англ. SDM)



V.10.2 Нидерланды – Стандарты информационной безопасности и защиты данных для фундаментального образования.

Министерство образования Нидерландов учредило Kennisnet в 2007 году. Kennisnet - это организация, интегрирующая информационные и коммуникационные технологии в учебные программы и предоставляющая широкий спектр образовательных ресурсов, инструментов образовательных технологий и информации, связанной с образованием.

В 2023 году Kennisnet опубликовала первую версию Рамочных стандартов информационной безопасности и защиты данных для фундаментального образования (Informatiebeveiliging en Privacy voor het Funderend Onderwijs, IBP FO). Эта система включает в себя конкретные примеры мер по защите школ от утечки данных или кибератак. Он помогает школам объективно контролировать уровень безопасности и защиты данных.

Эти рамочные стандарты включают раздел информационной безопасности, состоящий из 15 частей и 69 стандартов, и раздел защиты данных, который находится на стадии разработки и планируется к внедрению во втором полугодии 2023 года. Все образовательные учреждения должны внедрить эту систему к 2027 году.

V.10.3 Франция – Образовательный модуль для местных исполнительных органов

Французский орган по защите данных, известный как «Commission Nationale Informatique & Libertés» (CNIL), предлагает множество бесплатных ресурсов по соблюдению требований GDPR. В частности, Французский орган по защите данных (CNIL) недавно обновил свой образовательный модуль по работе с персональными данными граждан для местных исполнительных органов.[21]

Образовательный модуль для местных исполнительных органов охватывает следующие области:

- Использование индивидуальных камер сотрудниками муниципальной полиции.
- Ведение избирательного списка.
- Ведение записей актов гражданского состояния.
- Назначение местным сообществом своего сотрудника по защите данных (англ. DPO).
- Реализация процессинга в рамках политической коммуникации.
- Предоставление телеуслуг.
- Муниципальные реестр оповещения и защиты населения.
- Передача информации «уполномоченным третьим лицам».
- Материалы институциональной коммуникации.
- Материалы школьных и внеклассных мероприятий.
- В центре внимания - программы-вымогатели (ransomware): серьезная угроза для населения.
- Перепись населения.
- Социальные и медико-социальные материалы.
- Право на доступ к административным документам и защиту персональных данных.
- Контроль за парковками со стороны местного населения.

Предоставляя практические принципы и рекомендации, эти инициативы помогают преодолеть разрыв между законодательными требованиями и их конкретной реализацией, способствуя тем самым повышению подотчетности и прозрачности в деятельности по обработке данных. Поскольку цифровая среда продолжает развиваться, эти модели и принципы служат ценными ресурсами для организаций и учебных

[21] https://www.cnil.fr/fr/comprendre-le-rgpd/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie

заведений, стремящихся поддерживать стандарты защиты данных и соответствовать требованиям GDPR.

V.11. Заключение

При том что GDPR обеспечивает надежную основу для защиты данных, его эффективность заключается в его реализации. Из описанных шагов становится очевидным, что суть GDPR заключается не только в соблюдении нормативных требований, но и в формировании устойчивой культуры уважительного отношения к персональным данным. Такая культура играет ключевую роль в условиях перехода к эпохе, основанной на данных, когда данные приравниваются к ценному ресурсу. Однако, как и при любых других значительных преобразованиях, особенно в обширной и многогранной сфере государственного управления, здесь не обойтись без проблем.

Проблемы, с которыми сталкиваются государственные организации, перекликаются с более общими проблемами, связанными с объединением устаревших бюрократических систем с быстро развивающимися цифровыми ожиданиями. Технологический прогресс, предоставляя решения для эффективной обработки и хранения данных, одновременно создает потенциальные угрозы в виде кибератак и взломов. Но именно пересечение этих технологий с устоявшимися бюрократическими процессами зачастую представляет собой наиболее серьезную проблему. При попытках обеспечить бесшовную интеграцию требований GDPR, государственные органы сталкиваются как с материальными (финансовыми и технологическими), так и с нематериальными (культурными и административными) аспектами своей деятельности.

Различные стратегии, применяемые странами Европы, еще раз подчеркивают, что не существует «универсального» подхода к внедрению GDPR. Адаптивность и гибкость регулирования, позволяет странам корректировать свои стратегии с учетом конкретных обстоятельств, исторического контекста и моделей управления. Однако такая адаптивность порождает и проблему обеспечения согласованности стандартов в различных государственных структурах.

Важнейшим выводом из представленных примеров является всеобщее признание значимости GDPR. В каждой стране, будь то создание специальных должностей, обновление политик или применение строгих методик оценки, была продемонстрирована искренняя попытка соответствовать сути GDPR. Эти усилия, несмотря на их разнообразие, отражают глобальное стремление к повышению стандартов защиты данных, укреплению общественного доверия.

В более широком контексте, процесс внедрения GDPR в государственном управлении служит свидетельством эволюции взаимодействия между гражданами и их правительствами в цифровую эпоху. По мере того, как данные продолжают определять эту эволюцию, внимание к надежным мерам защиты информации будет только возрастать. Государственные органы, обеспечивая соответствие GDPR, не просто выполняют предписания, а подтверждают свои обязательства перед гражданами - обещание защищать их права, доверие и данные во все более взаимосвязанном мире.

В заключение следует отметить, что гармонизация законодательства с требованиями GDPR не только сопряжена с трудностями, но и открывает новые возможности. Это возможность для государственных органов перестроить свою работу, восстановить доверие общества и установить золотой стандарт защиты данных, ориентируясь при этом на все тонкости цифровой революции.

V.12. Список литературы

- BfDI. (n.d.). The standard data protection model. https://www.bfdi.bund.de/EN/Fachthemen/Inhalte/Technik/SDM.html
- CNIL (2022). Le MOOC de la CNIL est de retour dans une nouvelle version enrichie. https://www.cnil.fr/fr/comprendre-le-rgpd/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie
- CNPD (2022). GDPR - Certified Assurance Report based Processing Activities (CARPA) certification criteria (Version 1.0). https://cnpd.public.lu/content/dam/cnpd/fr/professionnels/certification/lu-gdpr-carpa-certificationscheme.pdf.
- CNPD (2022). Decision No. 15/2022. https://cnpd.public.lu/dam-assets/fr/professionnels/certification/decision-n-15-2022-du-13-mai-2022-criteres-de-certification.pdf
- ECCP (n.d.). Euro privacy Overview. https://www.europrivacy.org/en/ep/overview
- ECCP (n.d.). Euro privacy Criteria. https://www.europrivacy.org/en/ep/europrivacy-criteria
- EDPB. (2022). Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR certification criteria, adopted on 1 February 2022. https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-12022-draft-decision-luxembourg_en
- EDPB. (2022). Opinion 28/2022 on the Euro privacy criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5 (GDPR). https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282022-europrivacy-criteria-certification_en
- General Data Protection Regulation (GDPR). (2018). Art. 12 GDPR – Transparent Information, communication and modalities for the exercise of the rights of the data subject. https://gdpr-info.eu/art-12-gdpr/
- Kennisnet. (n.d.). Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs. https://aanpakibp.kennisnet.nl/normenkader/
- Kennisnet. (2023). Normenkader informatiebeveiliging en privacy.
- Kennisnet. (2023). Voorlopige starttabel 1.0 bij normenkader IBP.
- LfDI. (2022). Standard-Datenschutsmodell.
- https://www.datenschuts-mv.de/datenschuts/datenschutsmodell/.
- Martins, F., Amaral, L., & Ribeiro, P. (2020). Implementation of GDPR: Learning with a local administration case study. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 205-216. doi:10.1007/978-3-030-51005-3_19.
- Veale, M. (2018). Data Management and Use: Case Studies of Technologies and Governance [Preprint]. doi:10.31235/osf.io/rwgs9.

I. ISO/IEC 27001:2022

VI.1. Введение и обзор стандарта ISO/IEC 27001:2022

Стандарт ISO/IEC 27001 является наиболее авторитетным на международном уровне в качестве системы управления информационной безопасностью (СУИБ) для защиты конфиденциальности, доступности и целостности информационных активов организации. ISO/IEC 27001 представляет собой рамки, содержащие требования и элементы управления безопасностью для систематического создания и непрерывного функционирования процедур и процессов управления безопасностью, политики безопасности и т.д. с целью защиты информационных активов организации. Он позволяет преодолеть ограничения фрагментарного и разового управления за счет систематического и непрерывного функционирования системы управления. Стандарт помогает организациям понять, как определить политику и цели безопасности организации для укрепления информационной безопасности, внедрить необходимые средства контроля безопасности и поставить четкие задачи по снижению рисков. Приняв стандарт ISO 27001, организации могут администрировать правовые требования, например, регулярно проверять статус соответствия.

Активы, подлежащие защите, весьма обширны, включая не только цифровую информацию, но и физические активы, например, документы, поэтому одновременно должна осуществляться техническая защита системы, а также физическая и административная защита.

Система ISO 27001 помогает постоянно находить, устранять и улучшать систематические, физические и административные уязвимости, которые могут стать факторами угрозы. Стандарт ISO 27001 был впервые принят как BS7799, а после пересмотра в 1999 году, ISO (Международная организация по стандартизации) ввела его в действие в качестве международного стандарта ISO 27001:2005 в 2005 году. Кроме того, после пересмотра стандарта ISO 27001:2013 в 2013 году, он снова пересмотрен ISO 27001:2022 в 2022 году.

VI.2. Принципы и задачи

Принцип ISO 27001 заключается в защите трех аспектов информации: конфиденциальности, целостности и доступности. Для обеспечения этой защиты стандарт ISO 27001 направлен на постоянное повышение уровня безопасности путем создания, внедрения и поддержания СУИБ.

Это достигается с помощью цикла PDCA (планирование, реализация, контроль, корректировка). PDCA включает в себя основные виды деятельности полного цикла, которые могут стимулировать долгосрочные улучшения.

Рис. 24: Применение модели PDCA к процессам СУИБ.

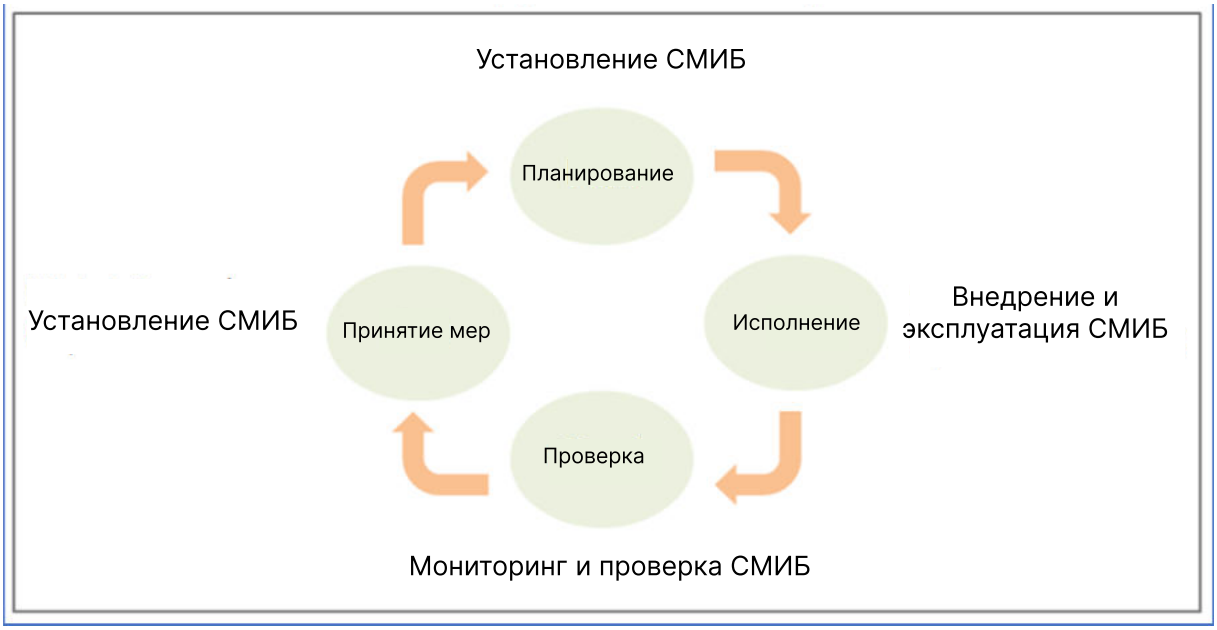


Таблица 13: Цикл PDCA, соотнесенный с стандартом ISO 27001.

Этапы	Пояснение
Планирование (Plan)	Разработка политик, целей, процессов и процедур СУИБ для повышения уровня информационной безопасности или управления рисками в соответствии с политиками и целями всей организации
Реализация (Do)	Внедрение и эксплуатация политик, средств контроля, процессов и процедур СУИБ
Контроль (Check)	Оценка политик, целей и практического опыта в области СУИБ, а также представление результатов измерений на рассмотрение руководства
Корректировка (Act)	Выполнение корректирующих и предупреждающих действий по результатам внутренних аудитов СУИБ, анализов со стороны руководства и другой информации для постоянного улучшения СУИБ

Ниже описан каждый этап цикла PDCA, соотнесенный со стандартом ISO 27001.

Планирование

Выявление потребностей заказчиков и заинтересованных сторон в области информационной безопасности и определение целей и политик СУИБ. Установление всех необходимых мероприятий по выявлению и устранению рисков и возможностей для достижения намеченных результатов в соответствии с политикой организации в области информационной безопасности.

Этому этапу соответствуют следующие четыре раздела из числа основных разделов ISO 27001. Каждый из этих разделов способствует созданию внутренней среды для внедрения ISO 27001.

Раздел 4. Контекст организации
Раздел 5. Лидерство
Раздел 6. Планирование
Раздел 7. Обеспечение

Реализация

Это этап выполнения плана. Он означает воплощение планов и разработок в жизнь. На этом этапе необходимо внедрить и задействовать установленные процессы и процедуры. Для успешного выполнения плана необходимо провести обучение и подготовку сотрудников, а также предоставить необходимое оборудование.

В стандарте ISO 27001 этому этапу соответствует один раздел.

Раздел 8. Функционирование

Контроль

На этом этапе проводится оценка внедрения и функционирования системы ISO 27001. Путем измерения и оценки результатов своих действий выявляются области для улучшения в области внедрения и функционирования, а также возникающие уязвимости и угрозы, с которыми может столкнуться организация. Оценка результатов деятельности обычно проводится в форме аудита.

В стандарте ISO 27001 этому этапу соответствует один раздел из числа основных разделов.

Раздел 9. Оценка результатов деятельности

Корректировка

В стандарте ISO 27001 имеется один раздел, который относится к этому этапу.

Мы проводим мероприятия по улучшению на основе информации о слабых местах и недостатках, выявленных на этапе «Контроль» (CHECK), например, результатов аудита. После этапа «Корректировка» (ACT) мы возвращаемся к целям и стратегиям, поставленным на начальном этапе планирования, и снова начинаем цикл «PDCA». С помощью этих циклов можно постоянно совершенствовать СУИБ.

Раздел 10. Улучшение

VI.3. Детальный анализ технических спецификаций и требований

Стандарт ISO 27001 представляет собой модель системы управления, которая обеспечивает применимые цели и меры контроля. Стандарт включает требования к процессам управления и требования к мерам контроля информационной безопасности.
Требования к процессам управления представлены семью разделами: **① Контекст организации, ② Лидерство, ③ Планирование, ④ Обеспечение, ⑤ Функционирование, ⑥ Оценка результатов деятельности** и **⑦ Улучшение.**

Требования к мерам контроля информационной безопасности включают 93 мероприятия в четырех категориях, согласно Приложению A «Цели и меры контроля».

Заявление о применимости (англ. SoA) публикуется на основе Приложения A.

- Организационные (37 мер контроля)
- Люди (8 мер контроля)
- Физические (14 мер контроля)
- Технологические (34 мер контроля)

Рис. 25: Требования к процессу управления информационной безопасностью

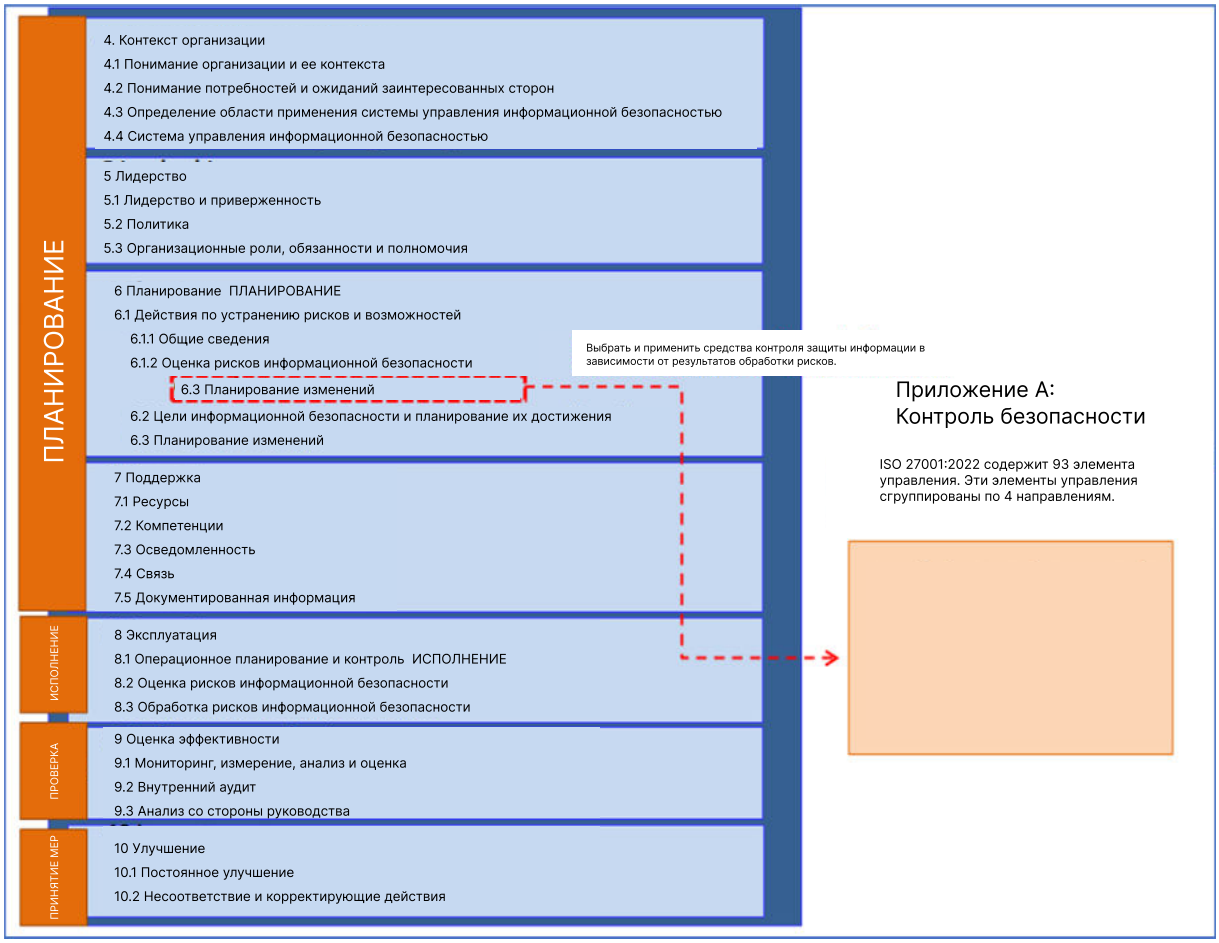


Таблица 14: Требование к процессу управления информационной безопасностью

Раздел	**Требование**
4. Контекст организации	4.1 Понимание организации и ее контекста. 4.2 Понимание потребностей и ожиданий заинтересованных сторон. 4.3 Определение области применения системы управления информационной безопасностью. 4.4 Система менеджмента информационной безопасностью.
5. Лидерство	5.1 Лидерство и обязательства 5.2 Политика. 5.3 Организационные функции, обязанности и полномочия.
6. Планирование	6.1 Действия по устранению рисков и реализации возможностей. 6.1.1 Общие положения. 6.1.2 Оценка рисков информационной безопасности. 6.1.3 Обработка рисков информационной безопасности. 6.2 Цели в области информационной безопасности и планирование их достижения. 6.3 Планирование изменений.
7. Поддержка	7.1 Ресурсы. 7.2 Компетентность. 7.3 Осведомленность. 7.4 Коммуникации. 7.5 Документированная информация. 7.5.1 Общие положения. 7.5.2 Создание и обновление. 7.5.3 Контроль документированной информации.

Раздел	Требование
8. Функциониро-вание	8.1 Оперативное планирование и контроль. 8.2 Оценка рисков информационной безопасности. 8.3 Обработка рисков информационной безопасности.
9. Оценка результатов деятельности	9.1 Мониторинг, измерение, анализ и оценка. 9.2 Внутренний аудит. 9.2.1 Общие положения. 9.2.2 Программа внутреннего аудита. 9.3 Анализ со стороны руководства 9.3.1 Общие сведения 9.3.2 Материалы для анализа со стороны руководства 9.3.3 Результаты анализа со стороны руководства
10.Улучшение	10.1 Непрерывное улучшение 10.2 Несоответствия и корректирующие действия

Таблица 15: Приложение A. Меры контроля информационной безопасности

Категория	Меры контроля
Организационная (37 средств контроля)	5.1 Политики в области информационной безопасности. 5.2 Роли и обязанности в области информационной безопасности. 5.3 Разделение обязанностей. 5.4 Обязанности руководства. 5.5 Контакты с государственными органами. 5.6 Контакты с группами по особым интересам. 5.7 Разведка угроз. 5.8 Информационная безопасность в управлении проектами. 5.9 Инвентаризация информационных и других связанных с ними активов. 5.10 Приемлемое использование информации и других связанных с ней активов. 5.11 Возврат активов. 5.12 Классификация информации. 5.13 Маркировка информации. 5.14 Передача информации. 5.15 Контроль доступа. 5.16 Управление идентификацией. 5.17 Информация об аутентификации. 5.18 Права доступа. 5.19 Информационная безопасность в отношениях с поставщиками. 5.20 Решение вопросов информационной безопасности в рамках соглашений с поставщиками. 5.21 Управление информационной безопасностью в цепочке поставок информационно-коммуникационных технологий (ИКТ). 5.22 Мониторинг, анализ и управление изменениями услуг поставщиков. 5.23 Информационная безопасность при использовании облачных сервисов. 5.24 Планирование и подготовка к управлению инцидентами информационной безопасности. 5.25 Оценка и принятие решений по событиям в области информационной безопасности. 5.26 Реагирование на инциденты информационной безопасности. 5.27 Обучение на основе инцидентов информационной безопасности. 5.28 Сбор доказательств. 5.29 Информационная безопасность при сбоях. 5.30 Готовность ИКТ к обеспечению непрерывности бизнеса. 5.31 Юридические, законодательные, нормативные и договорные требования. 5.32 Права на интеллектуальную собственность. 5.33 Защита записей. 5.34 Конфиденциальность и защита персональной идентифицируемой информации (PII). 5.35 Независимая экспертиза информационной безопасности.

Категория	Меры контроля
	5.36 Соблюдение политик, правил и стандартов информационной безопасности. 5.37 Документированные операционные (рабочие) процедуры.
Люди (8 мер контроля)	6.1 Скрининг. 6.2 Условия найма. 6.3 Информирование, обучение и подготовка кадров в области информационной безопасности. 6.4 Дисциплинарный процесс. 6.5 Обязанности после увольнения или смены места работы. 6.6 Соглашения о конфиденциальности или неразглашении информации. 6.7 Удаленная работа. 6.8 Отчетность о событиях информационной безопасности.
Физическая (14 мер контроля)	7.1 Физические периметры безопасности. 7.2 Физический вход. 7.3 Обеспечение безопасности офисов, помещений и сооружений. 7.4 Мониторинг физической безопасности. 7.5 Защита от физических и экологических угроз. 7.6 Работа в безопасных местах. 7.7 Политика чистого стола и экрана. 7.8 Размещение и защита оборудования. 7.9 Обеспечение безопасности активов, находящихся за пределами организации. 7.10 Средства хранения данных. 7.11 Вспомогательные коммуникации. 7.12 Защита кабелей. 7.13 Техническое обслуживание оборудования. 7.14 Обеспечение безопасной утилизации или повторного использования оборудования.
Технологическая (34 мер контроля)	8.1 Устройства конечных точек пользователя. 8.2 Права привилегированного доступа. 8.3 Ограничение доступа к информации. 8.4 Доступ к исходному коду. 8.5 Безопасная аутентификация. 8.6 Управление мощностями. 8.7 Защита от вредоносного ПО. 8.8 Управление техническими уязвимостями. 8.9 Управление конфигурацией. 8.10 Удаление информации. 8.11 Маскирование данных. 8.12 Предотвращение утечки данных. 8.13 Резервное копирование информации. 8.14 Резервирование средств обработки информации. 8.15 Ведение журнала. 8.16 Деятельность по непрерывному наблюдению. 8.17 Синхронизация часов. 8.18 Использование привилегированных служебных программ. 8.19 Установка программного обеспечения на операционные системы. 8.20 Безопасность сетей. 8.21 Безопасность сетевых сервисов. 8.22 Разделение сетей. 8.23 Веб-фильтрация. 8.24 Использование криптографии. 8.25 Жизненный цикл безопасной разработки. 8.26 Требования к безопасности приложений. 8.27 Архитектура и принципы проектирования защищенных систем. 8.28 Безопасное программирование. 8.29 Тестирование безопасности при разработке и приемке. 8.30 Аутсорсинг разработки.

Категория	Меры контроля
	8.31 Разделение сред разработки, тестирования и производства. 8.32 Управление изменениями. 8.33 Тестовая информация. 8.34 Защита информационных систем при проведении аудиторских проверок.

VI.4. Основной этап создания СУИБ.

Основными этапы при создании СУИБ:

Этап 1: Контекстный анализ

- Анализ внутренних и внешних (клиентских, юридических) вопросов, заинтересованных сторон и потребностей.
- Анализ состояния информационной безопасности организации. Анализ несоответствий между требованиями ISO 27001 и существующей системой безопасности.
- Определение области сертификации и идентификация активов.

Этап 2: Анализ и оценка рисков

- Установление и соблюдение критериев выполнения оценки рисков и критериев принятия рисков.
- Выявление рисков, связанных с потерей конфиденциальности, целостности и доступности информации.
- Оценка реалистичной вероятности реализации выявленных рисков и определение уровней риска.
- Сопоставление результатов анализа рисков с критериями риска и определение приоритетности проанализированных рисков для их обработки.

Этап 3: Обработка риска в соответствии с результатами оценки риска

- Определение всех мер контроля, необходимых для внедрения процедуры обработки рисков информационной безопасности.

Этап 4: Меры контроля информационной безопасности (цели и меры контроля Приложения А)

- Сравнение установленных мер контроля с мерами, перечисленными в Приложении А и проверка полноты необходимых мер контроля (что ни одна мера не упущена).
- Подготовка Заявления о применимости (англ. SoA), следующего содержания:
- · Необходимые меры контроля.
- · Обоснование включения или исключения мер контроля.
- · Внедрены ли необходимые меры контроля или нет.

Этап 5: Функционирование (функционирование и управление в соответствии с результатами оценки рисков)

- Планирование, внедрение и контроль процессов, необходимых для соответствия требованиям и выполнения действий, определенных на этапах 3 и 4.
- Организация проводит оценку рисков в запланированные интервалы времени, а также в случае, когда предлагаются или возникают существенные изменения.
- Организация внедряет план по управлению рисками.

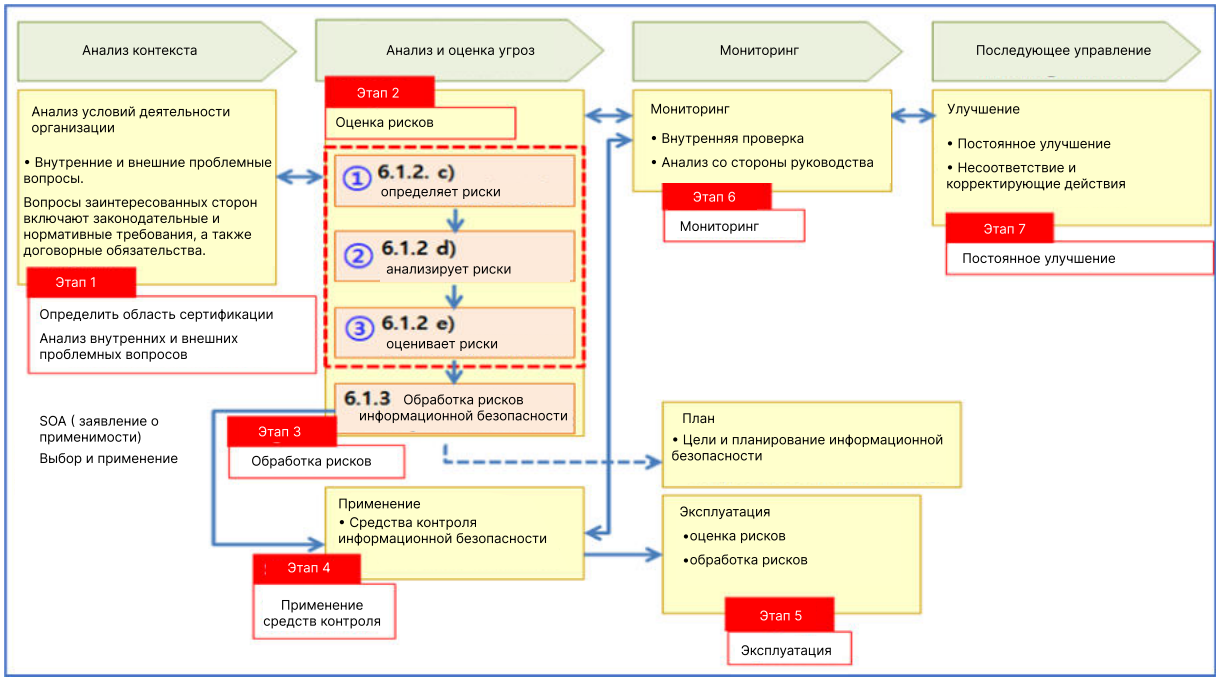
Этап 6: Мониторинг (внутренний аудит и мероприятия в рамках анализа со стороны руководства)

- Оценка эффективности с помощью мониторинга, измерений, внутреннего аудита, анализа со стороны руководства.

Этап 7: Последующее управление (пост-сертификационный аудит один раз в год)

- Постоянно улучшать пригодность, достаточность и эффективность системы управления информационной безопасностью, а при возникновении несоответствий предпринимать корректирующие действия.

Рис. 26: Основные этапы создания СУИБ.



VI.5. Обзор практических примеров использования

Ниже приведен пример результатов исследования, проведенного Юн-Чул Кангом и Джонг-Чанг Аном (англ. Youn-Chul Kang and Jong-Chang Ahn). Результаты показывают, что уровень информационной безопасности повысился в результате функционирования СУИБ на основе стандарта ISO 27001.

По мнению Юн-Чул Канга и Чон-Чан Ан, метод отбора компаний для анализа заключается в том, что сначала среди всех отечественных компаний, сертифицированных по стандарту ISO 27001, отбираются 38 компаний, которые могут собрать количественные данные, независимо от масштаба организации. В итоге отобраны пять организаций, связанных с финансовой деятельностью, которые могут предоставить данные.

Кроме того, компании, ставшие объектом анализа, первоначально прошли аудит в 2009 или 2010 году, а последующие аудиты были завершены к 2013 году в соответствии с трехлетним циклом сертификации.

В качестве измерительного показателя, основанного на «количестве несоответствий» в

отчёте о сертификационном аудите по ISO 27001:2005, использованном в исследовании Боэмера (англ. Boehmer's study), было статистически проанализировано, насколько уменьшается количество несоответствий, выявленных в ходе первоначального аудита после создания СУИБ в каждой компании, по мере ежегодного проведения последующего аудита.

В результате сравнительного анализа целевых компаний на предмет сертификации ISO 27001 было подтверждено, что количество случаев несоответствия снижалось каждый год в течение 3-летнего цикла от первоначального аудита во всех компаниях, получивших сертификат ISO 27001, как показано на рисунке ниже.

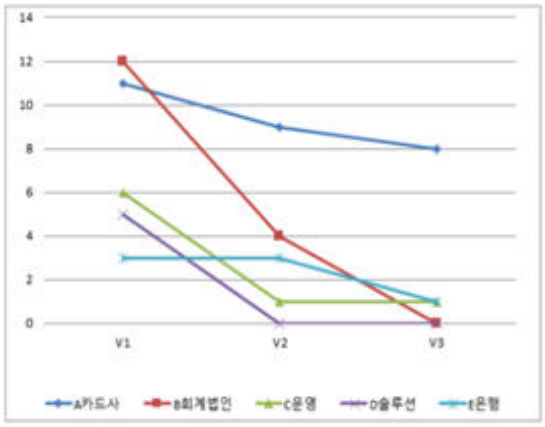
На рисунке ось X представляет собой первоначальную проверку (V1) и последующую проверку (V2, V3), а ось Y – количество выявленных случаев незначительных несоответствий. Анализируя полученные данные, можно сказать, что на основе стандарта первоначальной проверки было сделано минимум 27% и максимум 100% улучшений, при этом были обнаружены только несоответствия, рекомендации по улучшению или простые наблюдения, которые носят рекомендательный характер.

Рис. 27: Эффект от внедрения СУИБ на основе ISO 27001.

(Таблица) .

Анализ целевых организаций для улучшения влияние уровня информационной безопасности

Организация	Выручка (млн вон)	Количество работников	Количество сотрудников, работающих в сфере информационной безопасности в пределах сертификации
A	over 3,000,000	over 780	about 100
B	over 170,000	over 2,000	about 2
C	over 57,000	over 620	about 6
D	over 300,000	over 840	about 4
E	over 20,000,000	over 15,000	about 4



(Рис.) Тенденции по выявлению несоответствий после внедрения СМИБ

Источник: Юн-Чул Кан, Джонг-Чанг Ан (2018)

В отношении примеров в государственных учреждениях, можно рассмотреть внедрение стандарта ISO 27001 в Национальной службе научно-технической информации (англ. National Science and Technology Information Service, NTIS) и полученные результаты.

Согласно результатам исследования, проведенного Бён-Хи Ли, Иль-Ён Ё и Дже-Су Ким (англ. Byeong-Hee Lee, Il-Yeon Yeo, and Jae-Soo Kim), в случае NTIS, который является примером внедрения стандарта ISO 27001 в государственном учреждении, количество несоответствий и рекомендаций по улучшению уменьшилось в течение 3 лет после внедрения ISO 27001, как показано в таблице ниже.

Таблица 16: Изменение количества несоответствий и рекомендаций по улучшению

Год после внедрения	Существенные несоответствия	Незначительные несоответствия	Рекомендации по улучшению
1-й год	0 (2)	1 (19)	17 (7)
2-й год	0 (1)	0 (11)	11 (12)
3-й год	(0)	(0)	(8)

Источник: Бён-Хи Ли, Иль-Ён Ё, Дже-Су Ким (2011)

* В скобках указано число, полученное по результатам внутреннего аудита.
Кроме того, отмечается, что после внедрения ISO 27001 имели место следующие достижения и изменения:

- Изменился организационный КПЭ (ключевые показатели эффективности), которые стали более объективными.
- Уровень применения мер контроля информационной безопасности увеличился с 75% (100 позиций) в первый год до 79% (105 позиций) во второй год.
- Программа проверки безопасности распространилась на все ПК и расширилась на компании, обслуживающие резидентов.
- Полное внедрение систем контроля доступа к сети, таких как NAC, и внедрение системы управления безопасностью USB.
- Внедрение в организации защищенных принтеров/копировальных аппаратов.
- Применение эталонной модели данных (DRM) к сервису.
- Усиление управления информационными активами в организации.

Кроме того, относительно качественного результата отмечается повышение уровня осведомленности о безопасности, усиление обучения по вопросам безопасности и улучшение оценки надежности системы безопасности со стороны внешних организаций, таких как Национальная разведывательная служба (англ. National Intelligence Service).

VI.3.1 Конкретный реальный пример успешного внедрения ISO 27001 [22]

Компания «K» наняла способного менеджера по безопасности и успешно внедрила стандарт ISO 27001. Сначала менеджер по безопасности выявил все проблемы, включая организацию и способы решения, чтобы выработать правильные меры. Для решения выявленных проблем был создан отдел безопасности, выделены кадры и бюджет.

В первую очередь менеджер по безопасности сосредоточился на создании системы управления информационной безопасностью. Он специально показал руководству существующие риски компании и, по существу, убедил руководство в том, что компания не сможет устойчиво развиваться без инвестиций в информационную безопасность. Он подчеркнул, что если не создать систему управления информационной безопасностью, то велика вероятность повторного возникновения проблем, которые уже были решены. Руководство компании согласилось с этим мнением, и было принято решение о выделении инвестиций.

[22] Gil Min-kwon, “[Success Story] ISMS Introduction Case”, Daily Secu, May 29, 2013.

Организация работы персонала отдела безопасности на основе элементов ISO 27001 позволила уточнить должностные обязанности с тем, чтобы не допустить пробелов в работе. Кроме того, назначены аудиторы, чтобы поставленные задачи выполнялись эффективно. Перед началом фактической проверки проведена пробная проверка, чтобы проверить, есть ли пункты, требующие доработки. После получения сертификата ISO 27001 общая осведомленность об информационной безопасности повысилась.

По мере того, как области, которые можно решить административным путем, становятся ясными, решения по информационной безопасности могут внедряться только там, где это абсолютно необходимо, что снижает затраты. Работы по обеспечению информационной безопасности перешли от выполнения по инструкциям, к отдельной системе управления. Время, необходимое для обнаружения проблемы информационной безопасности и принятия мер по ее устранению, значительно сократилось. Кроме того, в процессе сертификации отдел безопасности смог понять общие системы и процессы компании, что позволило наладить взаимодействие с другими подразделениями.

VI.6. Преимущества внедрения стандарта ISO 27001

- Стандарт ISO 27001 помогает соблюдать законы и нормативные требования. Это снижает риск наложения штрафов или других санкций за несоблюдение требований.
- Получение сертификата ISO 27001 повышает не только внешний имидж компании, но и надежность, а также доверие клиентов, деловых партнеров к безопасности информации.
- Благодаря систематическому и непрерывному управлению рисками информационной безопасности можно постоянно повышать безопасность бизнеса и снижать риск несанкционированного доступа.
- Стандарт ISO 27001 позволяет создать систему управления безопасностью на очень узкоспециализированном уровне и всегда прорабатывать детали.
- Благодаря действию стандарта ISO 27001 можно заранее предотвратить развитие масштабных инцидентов безопасности, за счёт обнаружения реальных рисков и проблем информационной безопасности на ранней стадии.
- Доверие к информационной безопасности благодаря сертификации по международным стандартам облегчает выход бизнеса на мировые рынки.

В случае с услугами электронного правительства и государственного управления, если произойдет инцидент кибербезопасности, масштабы ущерба и последствия могут быть очень большими, поэтому важность обеспечения безопасности в этих областях возрастает еще больше.

Для того, чтобы преодолеть ограничения, связанные с фрагментарным, разовым, частичным управлением информационной безопасностью, ориентированным на неавтономное регулирование, необходимо внедрить систему управления ISO 27001. Внедрение системы ISO 27001 в услуги электронного правительства и государственного управления позволит заложить основу для непрерывного ежегодного повышения уровня информационной безопасности и кардинально улучшить уровень информационной безопасности за счет систематического управления. Кроме того, благодаря

сертификации по международному стандарту можно повысить внутреннюю и внешнюю надежность услуг электронного правительства и государственных служб.

VI.7. Ограничения и недостатки системы ISO 27001

- СУИБ призвана подтвердить, что бизнес-процессы по защите информации постоянно внедряются и соблюдаются, но стандарт не гарантирует, что это надёжная система, которую нельзя взломать.
- Для внедрения ISO 27001 требуются затраты и трудовые ресурсы, что может стать финансовой нагрузкой для организаций. Кроме того, требуются затраты и трудовые ресурсы для поддержания ISO 27001 в рабочем состоянии.
- ISO 27001 – это стандарт, который помогает организациям систематически управлять информационной безопасностью и улучшать ее, однако уровень информационной безопасности организации не повышается, если организация принимает только временные меры, чтобы пройти сертификационные аудиты.

VI.8. Рекомендации по эффективному применению и внедрению стандарта ISO 27001

- Поскольку система управления информационной безопасностью помогает обнаружить угрозы безопасности на ранней стадии и предотвратить происшествия, то ее целесообразно создавать и запускать как можно раньше. После того как система менеджмента информационной безопасностью создана и запущена, уровень безопасности организации можно повышать каждый год.
- Для успешного применения стандарта ISO 27001 в организации и повышения уровня информационной безопасности до надежного необходимы активная и твердая воля руководства и его участие в обеспечении информационной безопасности.
- Поскольку идеальной безопасности не существует, необходимо ежегодно минимизировать управленческие, технические и физические уязвимости, постоянно выделять бюджет и задействовать профессиональные кадры.
- Если специфика организации связана с применением новых технологий и особыми условиями, то система может быть усовершенствована путем применения новых мер контроля безопасности, соответствующих специфике организации, а также мер контроля безопасности, предлагаемых в стандарте ISO 27001.

Стандарт обеспечения кибербезопасности и конфиденциальности - ISO 29100

VII.1. Введение

VII.1.1 Важность кибербезопасности и конфиденциальности в современном цифровом пространстве

В современных условиях, когда на технологии полагаются все больше и больше, а конфиденциальные данные часто хранятся и передаются в Интернете, кибербезопасность и конфиденциальность приобретают все более важное значение. Кибератаки становятся все более изощренными и широко распространенными, что чревато такими серьезными последствиями, как финансовые потери, ущерб репутации и даже физический ущерб. О важности кибербезопасности и конфиденциальности свидетельствуют многочисленные громкие случаи утечки данных, произошедшие в последние годы, такие как утечка данных компании «Equifax» в 2017 году, в результате которой была раскрыта личная информация 143 млн. потребителей, взлом «SolarWinds» в 2020 году, в результате которого были взломаны сети множества государственных учреждений и частных компаний, а также недавние утечки данных компаний «T-Mobile», «Kroger», «California DMV», «Microsoft Exchange Server» и атака на компанию «Colonial Pipeline» в 2022 году в целях вымогательства. Помимо финансового и репутационного ущерба, который может быть нанесен в результате кибератаки, существуют также правовые и нормативные последствия. Во многих странах действуют законы и нормативные акты о защите данных, требующие от организаций защиты персональной информации клиентов и сотрудников, несоблюдение которых влечет за собой штрафы и судебные иски, например, Общий регламент защиты персональных данных Европейского союза (GDPR), согласно которому за несоблюдение требований по защите данных могут быть наложены штрафы в размере до 4% от мирового годового дохода компании.

Кроме того, люди все больше беспокоятся о своей конфиденциальности и о том, как их персональные данные используются компаниями и правительствами. Скандал с компанией «Cambridge Analytica» в 2018 году, когда данные миллионов пользователей «Facebook» были собраны без их согласия для использования в политической рекламе, подчеркнул необходимость повышения прозрачности и контроля за персональными данными.

Основные причины важности кибербезопасности и конфиденциальности в современном цифровом пространстве можно сформулировать следующим образом:

- ***Защита от киберугроз:*** киберугрозы, такие как хакерские атаки, утечки данных, атаки с использованием программ-вымогателей и кража персональных данных, становятся все более распространенными и изощренными. Для защиты конфиденциальной информации, включая персональные данные, финансовые документы, интеллектуальную собственность и средства обеспечения национальной безопасности, необходимы решительные меры по обеспечению кибербезопасности.

- ***Защита конфиденциальности:*** в эпоху цифровых технологий мы получаем большое количество персональных данных в результате различных действий в Интернете. Защита конфиденциальности обеспечивает контроль над данными и снижает риск несанкционированного доступа или неправомерного использования.
- ***Защита интересов бизнеса:*** кибератаки могут оказать существенное влияние на предприятия любого масштаба. Нарушение в области кибербезопасности может привести к финансовым потерям, ухудшению репутации, юридическим обязательствам и утрате доверия клиентов. Внедрение мер по обеспечению кибербезопасности помогает защитить ценные активы и информацию предприятия.
- ***Национальная безопасность:*** кибербезопасность тесно связана с национальной безопасностью. Системы критической инфраструктуры все больше зависят от цифровых технологий, и защита этих систем от киберугроз необходима для предотвращения сбоев, которые могут повлиять на общественную безопасность или национальную оборону.
- ***Соответствие нормативным требованиям по защите данных:*** для обеспечения соблюдения прав на неприкосновенность частной жизни и привлечения организаций к ответственности за защиту персональных данных правительства разных стран мира приняли нормативные акты по защите данных. Соблюдение этих норм необходимо для того, чтобы избежать штрафных санкций и продемонстрировать свою приверженность защите персональных данных клиентов.
- ***Укрепление доверия и уверенности клиентов:*** кибербезопасность и конфиденциальность имеют большое значение для поддержания доверия к цифровым услугам. Компании, уделяющие первостепенное внимание мерам кибербезопасности и соблюдению конфиденциальности, укрепляют доверие и повышают свою репутацию.
- ***Предотвращение киберпреступлений и мошенничества:*** меры кибербезопасности служат сдерживающим фактором для киберпреступников и мошенников. Надежные методы обеспечения безопасности затрудняют злоумышленникам использование уязвимостей и вредоносную деятельность в Интернете, что способствует защите физических лиц, бизнеса и общества в целом.

В нашем взаимосвязанном мире для защиты от киберугроз, защиты персональной информации и обеспечения национальной безопасности крайне важны эффективные меры по обеспечению кибербезопасности и конфиденциальности. В связи с растущей зависимостью от технологий и все более изощренными кибератаками как никогда важно внедрять эффективные методы обеспечения кибербезопасности для защиты нашей жизни в цифровом пространстве. Организации и физические лица должны предпринимать активные шаги по защите своих данных, а правительства - продолжать разрабатывать и применять законы, способствующие обеспечению кибербезопасности и конфиденциальности. Таким образом, мы сможем установить доверие, соблюдать законодательство по защите данных и бороться с киберпреступностью. Одним словом, кибербезопасность и конфиденциальность необходимы для того, чтобы ориентироваться и защищать нашу жизнь в меняющемся цифровом пространстве.

VII.2. Функции системы кибербезопасности и конфиденциальности для организации и страны

Рамки по обеспечению кибербезопасности и конфиденциальности представляют структурированный подход к управлению и снижению рисков кибербезопасности для организаций и стран. В них описываются необходимые политики, процедуры и технические меры для защиты от киберугроз и обеспечения соблюдения прав на неприкосновенность частной жизни. Ниже приводится подробное описание функций системы кибербезопасности и конфиденциальности:

- ***Оценка и управление рисками:*** проведение организациями и странами комплексной оценки рисков с целью выявления уязвимостей, угроз и потенциальных последствий. Данная мера позволяет им определять приоритетность рисков, эффективно распределять ресурсы и разрабатывать стратегии управления рисками для минимизации угроз и снижения вероятности и последствий киберинцидентов.
- ***Политики и процедуры:*** внедрение политик и процедур, которые регулируют сферу кибербезопасности и конфиденциальности. Данные политики определяют роли и обязанности, устанавливают принципы работы с данными, определяют порядок реагирования на инциденты, описывают программы повышения осведомленности о безопасности, а также обеспечивают соответствие законодательным и нормативным требованиям. Понятные политики способствуют согласованности действий и обеспечивают основу для принятия решений.
- ***Меры контроля и защиты безопасности:*** определение набора мер контроля и защиты, которые организации и страны должны применять для защиты своих сетей, систем и данных. Данные меры могут включать средства сетевой защиты, механизмы шифрования, контроль доступа, системы обнаружения вторжений, методы безопасного программирования и регулярное обновление системы безопасности. Они помогают организациям и странам защититься от киберугроз и обеспечить конфиденциальность информации.
- ***Реагирование на инциденты и восстановление:*** рекомендации по планированию и управлению реагированием на инциденты. В них описаны процессы оперативного обнаружения и реагирования на инциденты безопасности, смягчения их последствий, восстановления систем и данных. Они также предусматривают создание каналов связи, механизмов информирования об инцидентах и координации действий с соответствующими заинтересованными сторонами, такими как правоохранительные органы или национальные службы реагирования на компьютерные инциденты (англ. CERT).
- ***Осведомленность и обучение:*** система подчёркивает важность программ повышения осведомленности и обучения в области кибербезопасности. В рамках этих программ сотрудники, подрядчики и другие заинтересованные стороны знакомятся с передовым опытом, потенциальными рисками и своей ролью в обеспечении кибербезопасности и соблюдении конфиденциальности. Повышая осведомленность и накапливая знания, организации и страны могут создавать культуру, ориентированную на безопасность, и повышать свой уровень информационной безопасности.

- ***Соответствие нормативным требованиям:*** система помогает организациям и странам соответствовать требованиям применимых законов, нормативных актов и отраслевых стандартов в области кибербезопасности и конфиденциальности. Она обеспечивают основу для понимания и выполнения требований различных регулирующих органов, таких как правила защиты данных, отраслевые стандарты соответствия (например, Стандарт безопасности данных индустрии платежных карт) или национальные политики кибербезопасности. Выполнение требований по обеспечению соответствия помогает организациям и странам снизить правовые и репутационные риски.
- ***Непрерывное совершенствование:*** система способствует развитию культуры непрерывного совершенствования, уделяя особое внимание регулярному анализу, мониторингу и оценке мер безопасности. Вместе с тем, поощряет организации и страны следить за появляющимися угрозами и технологиями, обновлять политику и меры контроля, а также учитывать уроки, извлеченные из инцидентов, для повышения устойчивости к меняющимся рискам кибербезопасности.
- ***Сотрудничество и обмен информацией:*** система часто подчеркивает важность сотрудничества и обмена информацией между организациями и странами. Это способствует развитию партнерства между государственным и частным секторами, обмену оперативной информацией об угрозах, передовым опытом и извлеченными уроками, а также сотрудничеству в реагировании на киберинциденты. Такие совместные усилия способствуют укреплению общей системы кибербезопасности и конфиденциальности за счет использования коллективного опыта и ресурсов.

В целом, рамочный документ по обеспечению кибербезопасности и конфиденциальности содержит рекомендации и функции, позволяющие организациям и странам эффективно управлять рисками кибербезопасности, разрабатывать политики и процедуры, внедрять меры контроля безопасности, реагировать на инциденты, повышать осведомленность, обеспечивать соответствие требованиям, содействовать непрерывному совершенствованию, поддерживать сотрудничество и обмен информацией. Соблюдение данных требований помогает повысить устойчивость к внешним воздействиям, защитить конфиденциальную информацию и повысить общий уровень кибербезопасности и конфиденциальности.

VII.3. Общие сведения и контекст

VII.3.1 Представление концепции кибербезопасности и конфиденциальности; их значение в современном цифровом мире.

В современном взаимосвязанном мире, где технологии играют центральную роль практически во всех сферах нашей жизни, понятия «кибербезопасность» и «конфиденциальность» приобрели огромное значение. Под кибербезопасностью понимается защита компьютерных систем, сетей и данных от цифровых угроз, а под конфиденциальностью – контроль и защита персональной информации. По мере развития технологий и роста нашей зависимости от цифровых платформ необходимость обеспечения безопасности наших цифровых активов и соблюдения конфиденциальности приобретает первостепенное значение.

Кибербезопасность чрезвычайно важна, поскольку она защищает от киберугроз, которые могут нарушить конфиденциальность, целостность и доступность критически важной информации. С ростом числа киберпреступлений, таких как утечка данных, атаки с использованием программ-вымогателей и кража персональных данных, организации и физические лица сталкиваются с постоянно растущим риском финансовых потерь, ущерба репутации и даже правовых последствий. Эффективные меры кибербезопасности, включая надежную межсетевую защиту, строгие протоколы аутентификации и регулярные оценки безопасности, помогают защититься от злоумышленников, минимизировать уязвимости и обеспечить надежность цифровых систем.

Наряду с кибербезопасностью, конфиденциальность играет важнейшую роль в сохранении автономии и доверия в цифровом мире. Технологический прогресс обеспечил беспрецедентный сбор, анализ и использование персональных данных, что требует принятия мер по обеспечению ответственного обращения с ними. Нарушение конфиденциальности может привести к несанкционированному доступу к конфиденциальным данным, ущемлению личных свобод и подрыву доверия к организациям и цифровым сервисам. Сохранение конфиденциальности предполагает прозрачную работу с данными, получение информированного согласия, внедрение мер контроля безопасности и соблюдение действующих законов и нормативных актов.

Однако соблюдение баланса между кибербезопасностью и конфиденциальностью представляет собой сложную задачу. Соблюдение баланса позволяет обеспечить безопасное и этичное использование цифровых технологий, защитить права физических лиц и минимизировать риски. По мере того, как киберугрозы становятся все более изощренными, меры кибербезопасности должны постоянно адаптироваться и развиваться. Аналогичным образом, вопросы конфиденциальности требуют постоянного внимания и активных действий, направленных на защиту персональной информации без ущерба для преимуществ, получаемых от технологий, основанных на данных.

Формирование культуры кибербезопасности и соблюдение прав на неприкосновенность частной жизни имеют большое значение для физических лиц, организаций и общества в целом. Отдавая предпочтение надежным методам кибербезопасности и обеспечивая ответственное использование персональных данных, мы можем создать более безопасную и надежную цифровую среду, способствующую инновациям, укреплению доверия и защите прав граждан на неприкосновенность частной жизни и информационную безопасность.

VII.3.2 Обзор вызовов и угроз, связанных с кибербезопасностью и конфиденциальностью.

Сфера кибербезопасности и конфиденциальности сталкивается с широким спектром вызовов и угроз, которые продолжают развиваться по мере технического прогресса. К числу основных вызовов и угроз относятся:

- ***Кибератаки:*** сложные кибератаки, такие как вредоносное ПО, программы-вымогатели, фишинг и DDoS-атаки (распределенный отказ в обслуживании),

представляют значительный риск для организаций и физических лиц. Эти атаки могут привести к утечке данных, финансовым потерям, нарушению работы сервисов и нанесению репутационного ущерба.

- ***Инсайдерские угрозы:*** инсайдеры, имеющие привилегированный доступ к конфиденциальной информации, могут намеренно или непреднамеренно создавать бреши в системе безопасности. Внутренние злоумышленники могут похищать данные или манипулировать ими, а небрежные сотрудники могут неосознанно нарушать безопасность в результате неэффективных действий или недостаточной осведомленности.
- ***Соответствие нормативным требованиям:*** выполнение требований различных нормативных актов в области кибербезопасности и конфиденциальности, таких как Общий регламент защиты персональных данных Европейского союза (англ. GDPR) или Закон Калифорнии о защите персональных данных потребителей (англ. CCPA), может оказаться непростой задачей для организаций. Соблюдение этих требований предполагает понимание и реализацию конкретных мер информационной безопасности, методов обеспечения конфиденциальности, протоколов уведомления о нарушении конфиденциальности данных и механизмов получения согласия.
- ***Риски третьих сторон:*** организации часто полагаются на сторонних поставщиков, что создает потенциальные риски для безопасности и конфиденциальности. Слабые места в защите системах третьих сторон могут быть использованы злоумышленниками для получения несанкционированного доступа к критическим данным или системам.
- ***Быстро меняющаяся картина угроз:*** угрозы кибербезопасности постоянно эволюционируют, поскольку злоумышленники разрабатывают новые методы и используют новые технологии. Чтобы не отставать от них, требуется постоянный мониторинг, обмен данными об угрозах и проактивная оценка уязвимостей.
- ***Концепция использования собственных устройств сотрудников (англ. BYOD) и удаленная работа:*** широкое распространение концепции «использования собственных устройств сотрудников» (англ. Bring Your Own Device) и рост числа удаленных работ привели к появлению новых проблем в области информационной безопасности. Персональные устройства и удаленные подключения могут не иметь достаточных мер контроля информационной безопасности, что повышает риск несанкционированного доступа или раскрытия данных.
- ***Инсайдерская утечка данных:*** непреднамеренная или преднамеренная утечка конфиденциальных данных со стороны авторизованных пользователей по-прежнему остается актуальной проблемой. Это может происходить в результате небезопасного обмена файлами, некачественной обработки данных или недостаточного обучения и осведомленности.
- ***Безопасность облачных вычислений:*** организации, переходящие на облачные сервисы, сталкиваются с уникальными проблемами безопасности. Защита данных, контроль доступа и шифрование в облачных средах должны быть тщательно продуманы, чтобы снизить риск несанкционированного доступа, потери данных или уязвимости сервисов.
- ***Недостаточная осведомленность об информационной безопасности:*** человеческий фактор и недостаточная осведомленность пользователей в вопросах информационной безопасности представляют собой значительный риск

для общей системы безопасности. Сотрудники, не умеющие распознавать фишинговые письма, использовать надежные пароли и придерживаться лучших практик безопасности, могут непреднамеренно поставить под угрозу системы и данные организации.

- ***Угрозы искусственного интеллекта и Интернета вещей:*** растущая зависимость от искусственного интеллекта и распространение устройств Интернета вещей способствуют возникновению новых уязвимостей. Атаки с использованием искусственного интеллекта, алгоритмические ошибки и недостаточные протоколы безопасности в устройствах Интернета вещей могут подвергнуть киберугрозам критически важную инфраструктуру и персональные данные.

Организациям и физическим лицам крайне важно постоянно узнавать об этих проблемах и угрозах, принимать проактивные меры безопасности и сохранять бдительность для снижения рисков в условиях постоянно меняющейся ситуации в области кибербезопасности и конфиденциальности.

VII.4. Обсуждение необходимости разработки систем кибербезопасности и конфиденциальности для поддержки организаций в их деятельности по обеспечению кибербезопасности и конфиденциальности.

Системы кибербезопасности и конфиденциальности являются важнейшими ориентирами для организаций, обеспечивающими защиту их информационных активов и соблюдение применимого законодательства и нормативных требований. Эти системы обеспечивают структурированный подход к созданию надежных программ обеспечения кибербезопасности и конфиденциальности. Важность этих систем подчеркивается нижеследующими ключевыми аспектами:

- ***Комплексное управление рисками:*** систематизированный способ выявления, оценки и управления рисками, связанными с использованием технологий и обработкой конфиденциальной информации. Это помогает организациям понять уникальный ландшафт рисков и определить приоритеты в работе по их минимизации.
- ***Стандартизированные лучшие практики:*** лучшие практики, методологии и меры контроля, разработанные экспертами в области кибербезопасности и конфиденциальности. Эти рекомендации помогают организациям внедрять эффективные меры безопасности, контроля конфиденциальности и управления данными на основе отраслевых стандартов.
- ***Индивидуальный подход:*** системы могут быть адаптированы к конкретной отрасли, масштабу и уровню риска организации. Они представляют собой гибкую структуру, которая может быть адаптирована к уникальным потребностям организации при соблюдении установленных принципов и рекомендаций.
- ***Соответствие нормативным требованиям:*** многие системы включают в себя законодательные и нормативные требования для обеспечения соответствия. Они помогают организациям ориентироваться в сложных законах и нормативных актах, предоставляя рекомендации по защите данных, уведомлению о нарушениях, согласию пользователей и другим аспектам, связанным с конфиденциальностью.

- ***Повышение эффективности и результативности:*** внедрение системы позволяет оптимизировать деятельность организации в области кибербезопасности и конфиденциальности. Хорошо реализованная система способствует повышению эффективности, предоставляя дорожную карту для внедрения мер контроля, проведения оценки рисков и создания процедур реагирования на инциденты. Это позволяет организациям оптимизировать распределение ресурсов и поддерживать единую систему безопасности.
- ***Улучшение коммуникаций и взаимодействия:*** системы способствуют четкому взаимодействию между различными заинтересованными сторонами, включая руководителей, ИТ-персонал, юридические службы и аудиторов. Создается общий язык и понимание требований кибербезопасности и конфиденциальности, способствуя сотрудничеству между различными департаментами и дисциплинами.
- ***Непрерывное совершенствование:*** ключевым аспектом систем является их нацеленность на постоянное совершенствование. В них часто уделяется особое внимание регулярному анализу, мониторингу и оценке практики обеспечения информационной безопасности и конфиденциальности для выявления областей, требующих улучшения, и адаптации к изменяющимся угрозам и нормативным требованиям.
- ***Укрепление доверия и управление репутацией:*** внедрение надежной системы демонстрирует приверженность организации защите информационных активов и соблюдению конфиденциальности. Это может способствовать укреплению доверия со стороны клиентов, партнеров и заинтересованных сторон, а также сохранению репутации организации.
- ***Соответствие требованиям трансграничного законодательства:*** для организаций, ведущих трансграничную деятельность, платформы содержат рекомендации по управлению трансграничной передачи персональных данных и гармонизации практики в соответствии с требованиями различных юрисдикций. Это обеспечивает соблюдение различных законодательных требований при сохранении неизменного уровня безопасности и конфиденциальности.
- ***Бенчмаркинг и сертификация:*** многие системы предлагают внешние оценки и сертификацию организаций. Это обеспечивает независимое подтверждение практик организации в области кибербезопасности и конфиденциальности, позволяя им продемонстрировать соответствие требованиям и выделиться на рынке.

Системы кибербезопасности и конфиденциальности играют ключевую роль в деятельности организаций по защите цифровых активов и соблюдению требований конфиденциальности. Они обеспечивают структурированный подход, лучшие практики, руководство по соблюдению требований и систему непрерывного совершенствования, помогая организациям эффективно управлять рисками, обеспечивать соответствие нормативным требованиям и укреплять доверие в мире, который становится все более взаимосвязанным и основанным на данных.

VII.5. Обзор системы кибербезопасности и конфиденциальности

VII.5.1 Подробное объяснение системы кибербезопасности и конфиденциальности.

Рамки кибербезопасности и конфиденциальности – это организационный план (документ), устанавливающий рекомендации, лучшие практики и меры контроля для защиты информационных активов и обеспечения соответствия требованиям конфиденциальности. Такие рамки обеспечивают структурированный подход к управлению рисками кибербезопасности и конфиденциальности и позволяет организациям разрабатывать надежные программы безопасности. Ниже приводится подробное описание ключевых компонентов типовой системы кибербезопасности и конфиденциальности:

- ***Управление:*** система начинается с организации эффективного управления, которое предполагает определение ролей, обязанностей и ответственности за кибербезопасность и конфиденциальность в организации. Этот компонент включает создание политик, процедур и общих принципов, задающих тон в области информационной безопасности и конфиденциальности, а также обеспечивающих контроль и принятие решений.
- ***Оценка и управление рисками:*** в системе уделяется особое внимание проведению комплексной оценки рисков с целью выявления и определения приоритетности угроз, уязвимостей и потенциальных последствий. Организации оценивают риски, связанные с технологиями, системами, процессами и работой с конфиденциальными данными. Для минимизации или устранения выявленных рисков разрабатываются стратегии снижения рисков, такие как внедрение мер контроля и защиты.
- ***Меры контроля безопасности:*** в системе описывается набор мер контроля безопасности, основанных на лучших отраслевых практиках и нормативных требованиях, для защиты от распространенных угроз безопасности. Этот компонент включают различные аспекты, в том числе управление доступом, сетевую безопасность, укрепление системы, реагирование на инциденты, шифрование данных, обучение сотрудников и меры физической безопасности. Система помогает организациям выбрать, внедрить и поддерживать соответствующие меры контроля, отвечающие их специфическим потребностям.
- ***Защита конфиденциальности:*** конфиденциальность является одним из важнейших аспектов системы. Этот компонент включает принципы и рекомендации по защите конфиденциальности, обеспечивающие соблюдение соответствующих законов и нормативных актов в области защиты конфиденциальности. В системе рассматриваются вопросы сбора данных, механизмов получения согласия, процедур обработки данных, хранения данных, прав субъектов данных и протоколов уведомления о нарушениях. При разработке и внедрении систем и процессов поощряются подходы, основанные на принципах конфиденциальности.
- ***Реагирование на инциденты и восстановление:*** в система особое внимание уделяется разработке плана реагирования на инциденты для эффективного обнаружения, реагирования и восстановления после инцидентов кибербезопасности. Этот компонент включает определение ролей и обязанностей, процедур эскалации инцидентов и протоколов взаимодействия. Кроме того, в

рамках системы особое внимание уделяется извлечению уроков из инцидентов путем анализа ситуации после инцидента с целью повышения уровня безопасности организации.

- ***Обучение и повышение осведомленности:*** в системе признается важность постоянного обучения и повышения осведомленности сотрудников о передовых методах обеспечения кибербезопасности и конфиденциальности. Организациям рекомендуется внедрять информационные кампании, проводить регулярные тренинги и предоставлять ресурсы для развития культуры безопасности и конфиденциальности среди всего персонала.
- ***Постоянный мониторинг и совершенствование:*** в системе подчеркивается необходимость постоянного мониторинга систем, сетей и данных для обнаружения возникающих угроз и реагирования на них. В соответствии с ней организациям рекомендуется внедрять средства контроля безопасности для мониторинга событий, проведения оценки уязвимостей, тестирования на проникновение и отслеживания соблюдения установленных политик и процедур. Для оценки эффективности программы безопасности и выявления областей, требующих улучшения, проводятся регулярные аудиты и обзоры.
- ***Соответствие требованиям и отчетность:*** система помогает организациям понять и соблюдать применимые законы, нормативные акты, отраслевые стандарты и договорные обязательства. Этот компонент помогает создать механизмы периодической отчетности и оценки соблюдения соответствующих требований кибербезопасности и конфиденциальности.
- ***Работа с поставщиками и третьими сторонами:*** в системе рассматриваются риски, связанные с привлечением сторонних поставщиков, и предоставляет рекомендации по оценке и управлению их безопасностью и конфиденциальностью. Этот компонент включает договорные обязательства, процессы комплексной проверки и механизмы постоянного мониторинга для обеспечения безопасности и конфиденциальности общих данных и систем.
- ***Непрерывность бизнеса и аварийное восстановление:*** в системе признается необходимость планирования непрерывности бизнеса и аварийного восстановления в случае инцидентов, связанных с кибербезопасностью. Этот компонент помогает организациям разработать стратегии и процессы, обеспечивающие доступность и целостность критически важных систем и данных во время и после киберинцидентов.

В целом система кибербезопасности и конфиденциальности предоставляет организациям систематический и целостный подход к защите информационных активов, снижению рисков, обеспечению соблюдения конфиденциальности и эффективному реагированию на инциденты кибербезопасности. система закладывает основу для создания устойчивой и безопасной среды, позволяя организациям адаптироваться к меняющимся угрозам и нормативным требованиям.

VII.5.2 Рамочный стандарт обеспечения кибербезопасности.

1) Стандарт обеспечения кибербезопасности НИСТ

Стандарт обеспечения кибербезопасности НИСТ (англ. NIST Cybersecurity Framework) – это общепризнанное руководство, предоставляющее организациям гибкий и стандартизированный подход к управлению и снижению рисков кибербезопасности. Стандарт создан Национальным институтом стандартов и технологий США (далее – НИСТ), который является федеральным агентством в составе Министерства торговли США, не обладающим регуляторными функциями, в ответ на указ президента США 2013 года. Этот стандарт является добровольной платформой для организаций всех уровней и отраслей, позволяющим им повысить уровень кибербезопасности.

Стандарт кибербезопасности НИСТ состоит из трех основных компонентов:

- ***Ядро системы:*** это пяти параллельных и непрерывных функций: Идентификация, защита, обнаружение, реагирование и восстановление.
  - *Идентификация:* направлена на понимание активов организации, выявление рисков кибербезопасности и разработку стратегии управления рисками. Эта функция предполагает проведение инвентаризации активов, оценку уязвимостей и понимание возможного влияния рисков кибербезопасности на бизнес-операции.
  - *Защита:* содержит рекомендации по внедрению мер защиты критически важных активов от угроз кибербезопасности. Эта функция включает такие меры, как контроль доступа, шифрование данных, безопасные конфигурации, программы обучения и повышения осведомленности, а также постоянное управление уязвимостями.
  - *Обнаружение:* направлено на внедрение систем и процессов, позволяющих выявлять и своевременно обнаруживать инциденты кибербезопасности. Эта функция включает мониторинг сетей и систем, проведение анализа угроз и внедрение механизмов обнаружения вторжений.
  - *Реагирование:* помогает организациям разрабатывать и реализовывать стратегии реагирования для эффективной минимизации последствий инцидентов кибербезопасности. Эта функция включает разработку плана реагирования на инциденты, определение ролей и обязанностей, а также проведение ретроспективного анализа для понимания характера и масштаба инцидентов.
  - *Восстановление:* направлено на восстановление операций и сервисов после инцидента кибербезопасности. Эта функция включает разработку планов и стратегий восстановления систем, восстановление данных из резервных копий и проведение анализа после инцидента для предотвращения подобных инцидентов в будущем.

- ***Уровни внедрения стандарта:*** уровни внедрения дают возможность организациям оценить текущее состояние кибербезопасности и поставить цели по повышению ее уровня. В зависимости от уровня управления рисками кибербезопасности организации подразделяются на четыре уровня (частичный, риск-ориентированный, повторяющийся и адаптивный).

- ***Профиль стандарта:*** профиль стандарта позволяет организациям создать дорожную карту для приведения в соответствие своих практик и целей в области кибербезопасности с желаемыми результатами. Предполагается построение профиля путем выбора и определения приоритетности конкретных целей, видов деятельности и ссылок в рамках ядра системы.

Рис. 28: Ядро системы кибербезопасности НИСТ

Благодаря своей практичности и масштабируемости стандарт кибербезопасности НИСТ (англ. НИСТ Cybersecurity Framework) получил широкое распространение и признание во всем мире. Стандарт используется не только организациями в США, но и служит ориентиром для других стран и отраслей при разработке своих стандартов и систем кибербезопасности.

1) ISO 27001

ISO 27001 — это международно признанный стандарт для систем управления информационной безопасностью (СУИБ). Стандарт предоставляет организациям основу для создания, внедрения, поддержания и постоянного совершенствования эффективной системы управления информационной безопасностью. Ниже приводится подробное описание стандарта ISO 27001:

- ***Область применения и контекст:*** стандарт ISO 27001 определяет область применения СУИБ, определяя границы и применимость системы управления информационной безопасностью в организации. В нем подчеркивается необходимость учета внутреннего и внешнего контекста, включая правовые, нормативные и договорные требования, а также риски для информационной безопасности организации.
- ***Лидерство и приверженность:*** стандарт подчеркивает важность лидерства и приверженности высшего руководства информационной безопасности.

VII.5.3 Рамочный стандарт обеспечения конфиденциальности.

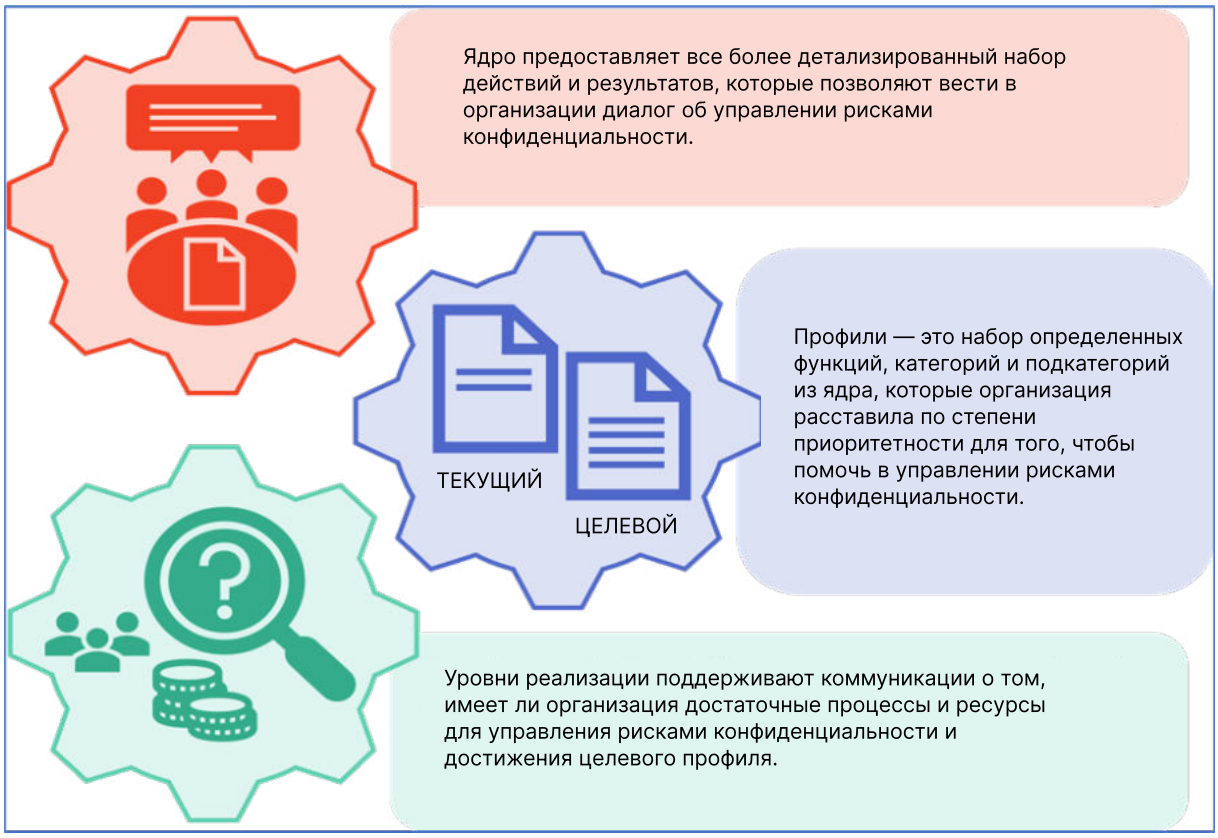
1) Стандарт обеспечения конфиденциальности НИСТ

Стандарт обеспечения конфиденциальности НИСТ (англ. NIST Privacy Framework) – это руководство, разработанное Национальным институтом стандартов и технологий (далее – НИСТ) с тем, чтобы помочь организациям эффективно управлять рисками конфиденциальности и включать вопросы конфиденциальности в общие процессы управления рисками. Ниже приводится подробное описание документа системы обеспечения конфиденциальности НИСТ:

- ***Ядро системы:*** ядро стандарта обеспечения конфиденциальности (англ. Privacy Framework Core) состоит из пяти ключевых функций, которые аналогичны функциям стандарта обеспечения кибербезопасности НИСТ:
  - *Идентификация:* организациям рекомендуется понять и расставить приоритеты в отношении рисков конфиденциальности, определив типы собираемых ими данных, цели их сбора и связанные с ними риски конфиденциальности.
  - *Управление:* направлено на создание и внедрение комплексной структуры управления конфиденциальностью в организации. Эта функция включает определение ролей и обязанностей, распределение полномочий по принятию решений, разработку политик и процедур для ведения деятельности, связанной с конфиденциальностью.
  - *Контроль:* предполагает реализацию соответствующих мер защиты конфиденциальности для минимизации выявленных рисков. Эта функция включает разработку и внедрение мер контроля конфиденциальности, таких как минимизация данных, контроль доступа и меры по защите данных, для снижения рисков конфиденциальности.
  - *Коммуникация:* подчеркивает важность прозрачности и эффективной коммуникации с лицами, чьи персональные данные собираются. Организации должны предоставлять четкие уведомления о конфиденциальности, информировать людей об их правах на конфиденциальность и создавать каналы для реализации их предпочтений в отношении конфиденциальности.
  - *Защита:* направлена на реализацию мер по эффективному реагированию на инциденты и нарушения конфиденциальности. Эта функция включает разработку планов реагирования на инциденты, проведение оценок воздействия на конфиденциальность (англ. PIA), а также создание процессов обнаружения, реагирования и восстановления после нарушения конфиденциальности.
- ***Профили:*** стандарт обеспечения конфиденциальности НИСТ позволяет организациям создавать профиль конфиденциальности. Профили помогают организациям привести свою деятельность, связанную с конфиденциальностью, в соответствие с бизнес-целями, приемлемым для организации уровнем риска и законодательными/нормативными требованиями. Профиль конфиденциальности может быть создан путем выбора и определения приоритетов соответствующих результатов и видов деятельности из ядра стандарта обеспечения конфиденциальности.

- ***Уровни реализации:*** как и стандарт кибербезопасности НИСТ, стандарт обеспечения конфиденциальности НИСТ включает уровни реализации, которые помогают организациям оценить степень зрелости их правил и процедур в отношении обеспечения конфиденциальности. Уровни включают «частичный», «риск-ориентированный», «повторяющийся» и «адаптивный», что отражает различные уровни управления рисками конфиденциальности и интеграции программ.

Рис. 29: Компоненты стандарта обеспечения конфиденциальности НИСТ



Стандарт обеспечения конфиденциальности НИСТ разработан с учетом требований адаптации и масштабирования, что делает его пригодным для организаций различных масштабов и отраслей. Стандарт способствует применению риск-ориентированного подхода к управлению конфиденциальностью, позволяя организациям систематически и всесторонне выявлять и устранять риски, связанные с конфиденциальностью.

2) ISO 29100

ISO/IEC 29100 – это международный стандарт, обеспечивающий основу для защиты конфиденциальности персональной идентификационной информации (далее – ПИИ). В нем изложены принципы защиты конфиденциальности и подчеркивается необходимость создания в организациях программы управления конфиденциальностью. Стандарт разграничивает роли контроллера и обработчика ПИИ и определяет их ответственность за защиту ПИИ. В стандарте также подчеркивается важность предоставления четких уведомлений о конфиденциальности, получения согласия на обработку ПИИ и признания прав физических лиц в отношении их ПИИ. Стандарт ISO/IEC 29100 решает проблемы,

связанные с трансграничной передачей данных, и способствует применению проактивного подхода к управлению конфиденциальностью.

Ниже подробно представлены некоторые ключевые аспекты ISO/IEC 29100:

- ***Принципы конфиденциальности ПИИ:*** стандарт описывает набор принципов конфиденциальности, которые служат основой для управления ПИИ. Эти принципы включают подотчетность, точность, согласие, определение цели, ограничение сбора, использования, раскрытия, хранения и ответственность за последующую передачу.
- ***Управление конфиденциальностью:*** стандарт ISO/IEC 29100 подчеркивает необходимость создания в организациях программы управления конфиденциальностью. Это предполагает определение ролей и обязанностей, разработку политик и процедур, проведение оценок воздействия на конфиденциальность (англ. PIA) для выявления рисков, связанных с конфиденциальностью, а также создание механизмов постоянного мониторинга и анализа.
- ***Роли ПИИ-контроллера и ПИИ-обработчика:*** стандарт разграничивает роли контроллера и обработчика ПИИ. Контроллер ПИИ отвечает за определение целей и средств обработки ПИИ, а обработчик ПИИ обрабатывает ПИИ от имени контроллера. ISO/IEC 29100 определяет ответственность и обязательства каждой роли в отношении защиты ПИИ.
- ***Уведомление о конфиденциальности:*** стандарт подчеркивает важность предоставления четких и прозрачных уведомлений о конфиденциальности лицам, чьи данные собираются. В нем указаны элементы, которые должны быть включены в уведомление о конфиденциальности, такие как идентификационные данные (личность) ПИИ контролера, цели обработки, категории получателей и права человека в отношении его ПИИ.
- ***Согласие:*** в стандарте ISO/IEC 29100 рассматривается вопрос получения согласия на обработку ПИИ. Он подчеркивает, что согласие должно быть добровольным, информированным и конкретным. Стандарт содержит рекомендации по получению, регистрации и управлению согласием в соответствии с требованиями конфиденциальности.
- ***Индивидуальное участие:*** стандарт признает права физических лиц в отношении их ПИИ. В нем подчеркивается важность обеспечения механизмов доступа, исправления, удаления и ограничения обработки ПИИ. ISO/IEC 29100 также подчеркивает, что организации должны эффективно обрабатывать запросы и жалобы физических лиц, касающиеся их ПИИ.
- ***Трансграничные потоки данных:*** в стандарте рассматриваются проблемы, связанные с международной передачей ПИИ. В нем подчеркивается необходимость обеспечения соответствия трансграничной передачи данных действующим законам и нормативным актам. Стандарт ISO/IEC 29100 содержит рекомендации по оценке достаточности защиты в стране-получателе и созданию соответствующих гарантий при передаче.

В целом, стандарт ISO/IEC 29100 служит основой для организации мер по защите персональных данных и соблюдения законов и нормативных актов в области защиты персональных данных. Он способствует проактивному подходу к управлению конфиденциальностью, помогая организациям укреплять доверие к людям и демонстрировать свою приверженность защите личной информации.

VII.6. Сравнение различных стандартов кибербезопасности и конфиденциальности

Стандарт кибербезопасности НИСТ и ISO 27001 — это системы управления рисками кибербезопасности. Стандарт кибербезопасности НИСТ является набором рекомендаций по снижению организационных рисков кибербезопасности, опубликованный НИСТ на основе существующих стандартов, руководств и практик. ISO 27001 – это международный стандарт, определяющий требования к созданию, внедрению, поддержанию и постоянному совершенствованию системы управления информационной безопасностью (СУИБ) в рамках организации.

Стандарт обеспечения конфиденциальности НИСТ и ISO 29100 — это система и стандарт управления рисками конфиденциальности. Стандарт обеспечения конфиденциальности НИСТ является добровольным инструментом, разработанным в сотрудничестве с заинтересованными сторонами и призванным помочь организациям в определении и управлении рисками конфиденциальности для создания инновационных продуктов и услуг при защите частной жизни. Стандарт ISO 29100 представляет собой систему управления конфиденциальностью, которая устанавливает общую терминологию конфиденциальности, определяет участников и их роли в обработке ПИИ, описывает вопросы обеспечения конфиденциальности и содержит ссылки на известные принципы конфиденциальности в области информационных технологий.

Стандарт кибербезопасности НИСТ и ISO 27001 способствуют целостному подходу к информационной безопасности, а система обеспечения конфиденциальности НИСТ и ISO 29100 содержат рекомендации по управлению рисками, связанными с конфиденциальностью. В зависимости от конкретных потребностей и требований организации могут использовать эти документы для совершенствования своих методов обеспечения безопасности и конфиденциальности. Важно отметить, что эти системы не являются взаимоисключающими и могут использоваться совместно для обеспечения комплексной защиты как от рисков кибербезопасности, так и от рисков конфиденциальности. Ниже приведена таблица для сравнения различных систем обеспечения кибербезопасности и конфиденциальности.

VII.7. Практические примеры

VII.7.1. Реальные примеры организаций, успешно внедривших системы обеспечения кибербезопасности и конфиденциальности.

Ниже приведены несколько реальных примеров организаций, успешно внедривших системы кибербезопасности и конфиденциальности:

1) Cisco Systems

Cisco Systems, ведущая технологическая компания, приняла систему кибербезопасности НИСТ для управления рисками кибербезопасности и совершенствования своей программы кибербезопасности. Согласно информации из Белой книги (англ. white paper), Cisco принимает систему кибербезопасности НИСТ, выстраивая свои продукты и услуги в области кибербезопасности в соответствии с функциями и категориями данной системы. В документе объясняется, как Cisco Secure может поддерживать каждую из пяти функций системы: идентификация, защита, обнаружение, реагирование и восстановление.

Например, в рамках функции «идентификация» компания Cisco Secure предлагает такие решения, как Cisco Secure Endpoint, Cisco Secure Malware Analytics и Cisco Umbrella SIG, которые помогают организациям выявлять и управлять рисками кибербезопасности. В рамках функции «защита» компания Cisco Secure предлагает такие решения, как Cisco Secure Firewall и Cisco Secure Workload, которые помогают организациям защитить свои системы и данные от киберугроз.

Аналогичным образом, в рамках функции «обнаружение» компания Cisco Secure предлагает такие решения, как Cisco Secure Firewall Threat Defence и Cisco Secure Network Analytics, которые помогают организациям обнаруживать киберугрозы и реагировать на них в режиме реального времени. В рамках функции «реагирование» компания Cisco Secure предлагает такие решения, как Cisco Secure Email и Cisco Secure Web Gateway, которые помогают организациям реагировать на киберинциденты и минимизировать их последствия. Наконец, в рамках функции «восстановление» компания Cisco Secure предлагает такие решения, как Cisco Secure Services, которые помогают организациям восстанавливаться после киберинцидентов и восстанавливать свои системы и данные.
В соответствии с требованиями системы обеспечения кибербезопасности НИСТ компания Cisco предоставляет полный портфель продуктов и услуг в области кибербезопасности, которые соответствуют функциям и категориям системы. Такой подход помогает организациям эффективно управлять рисками кибербезопасности и повышать общий уровень защиты.

1) Microsoft

Компания Microsoft внедрила систему кибербезопасности НИСТ для управления рисками кибербезопасности и совершенствования своей программы кибербезопасности. Согласно заявлению Microsoft, компания поддерживает систему кибербезопасности НИСТ и разработала решения для каждой из пяти основных функций системы: Идентификация, защита, обнаружение, реагирование и восстановление. Эти решения включают в себя управление активами, оценку рисков, контроль доступа, защиту данных, обнаружение аномалий, планирование мер по реагированию и восстановлению.

Облачные сервисы Microsoft прошли независимые аудиты на предмет соответствия требованиям Федеральной программа управления рисками и авторизацией (англ. FedRAMP) умеренного и высокого уровня и сертифицированы в соответствии со стандартами программы FedRAMP. Система кибербезопасности НИСТ ссылается на всемирно признанные стандарты, включая стандарт НИСТ 800-53 Контроль безопасности и конфиденциальности для информационных систем и организаций (англ. НИСТ SP 800-53 Privacy Controls for Information Systems and Organisations).

Таблица 17: Сравнение различных систем обеспечения безопасности

Рамочный стандарт	**Описание**	**Основные функции**	**Сильные стороны**	**Слабые стороны**
Система кибер-безопасности НИСТ (англ. NIST Cybersecurity Framework)	Добровольная система, разработанная Национальным институтом стандартов и технологий (англ. НИСТ) для помощи организациям в управлении и снижении риска кибербезопасности.	Идентификация, защита, обнаружение, реагирование, восстановление.	Обеспечивает общий язык и системную методологию управления рисками кибербезопасности. Обеспечивает экономически эффективную расстановку приоритетов и передачу информации о мероприятиях по улучшению среди заинтересованных сторон организации.	Некоторые организации могут столкнуться с трудностями при внедрении системы из-за личного сопротивления или дополнительных затрат. Концепция не отражает современных подходов к облачным вычислениям.
ISO 27001	Международный стандарт, определяющий требования к созданию, внедрению, поддержанию и постоянному совершенствованию системы менеджмента информационной безопасностью (СУИБ).	Конфиденциальность, целостность, доступность.	Обеспечивает целостный подход к информационной безопасности: проверка людей, политик и технологий. Помогает организациям осознать риски, проактивно выявлять и устранять слабые места.	Некоторые организации могут столкнуться с трудностями при его внедрении из-за большого количества категорий и подкатегорий.
Система обеспечения конфиденциальности НИСТ (англ. NIST Privacy Framework)	Добровольный инструмент, разработанный НИСТ в сотрудничестве с заинтересованными сторонами и призванный помочь организациям в определении и управлении рисками, связанными с конфиденциальностью, для создания инновационных продуктов и услуг при этом обеспечивая конфиденциальность.	Конфиденциальность, целостность, доступность.	Обеспечивает общий язык для управления рисками конфиденциальности. Позволяет организациям определить области, в которых можно усилить существующие процессы или внедрить новые. Позволяет усилить коммуникацию в рамках всей организации.	Система не отражает современных подходов к облачным вычислениям. Система не является предписывающим подходом, основанным на требованиях.

Рамочный стандарт	Описание	Основные функции	Сильные стороны	Слабые стороны
ISO 29100	Международный стандарт, обеспечивающий основы конфиденциальности, в котором указана общая терминология конфиденциальности; определены участники и их роли в обработке персонально идентифицируемой информации (ПИИ); описаны соображения защиты конфиденциальности; приведены ссылки на известные принципы конфиденциальности для информационных технологий.	Не указано.	Обеспечивает общую терминологию конфиденциальности и определяет роли участников процесса обработки ПИИ. Помогает организациям управлять рисками, связанными с безопасностью данных, принадлежащих компании или обрабатываемых ею. Соблюдает все лучшие практики и принципы, закрепленные в настоящем Международном стандарте.	Стандарт не содержит формальных требований, которым компания должна следовать.

В дополнение к этому Microsoft разработала матрицу ответственности заказчика по системе обеспечения кибербезопасности НИСТ, в которой перечислены все требования к мерам контроля, зависящие от реализации заказчиком, мерам контроля с общей ответственностью, а также подробная информация относительно реализации мер контроля, принадлежащих Microsoft. Клиенты могут скачать матрицу из раздела Service Trust Portal Blueprints в подразделе НИСТ CSF Blueprints.

В целом внедрение компанией Microsoft системы кибербезопасности НИСТ свидетельствует о ее стремлении управлять рисками кибербезопасности и защищать информационные активы своих клиентов.

3) Округ Арлингтон, штат Вирджиния

Округ Арлингтон (штат Вирджиния) столкнулся с рядом проблем, таких как неактуальное регулирование, которое не успевает за стремительным появлением новых типов персональной информации, ограниченность ресурсов для местных исполнительных органов в области управления нерегулируемой персональной информацией, низкий уровень грамотности в вопросах конфиденциальности и малое количество компетентных специалистов в области конфиденциальности среди сотрудников.

Правительство округа Арлингтон осуществило ряд проектов, таких как создание межведомственной Рабочей группы по конфиденциальности данных для разработки принципов конфиденциальности, политики, оценки воздействия и обучения, экспериментальной практики реализации программ конфиденциальности в рамках пилотных технологических программ «умный город», создание академических/общественных групп по конфиденциальности для обеспечения независимой, добровольной обратной связи и надзора за соблюдением требований по управлению рисками конфиденциальности, разработка оценки воздействия конфиденциальности на конкретные проекты и планов по снижению рисков в соответствии с подкатегориями системы обеспечения конфиденциальности НИСТ.

В результате повысилась грамотность сотрудников и населения в вопросах конфиденциальности, улучшилось взаимодействие с населением благодаря использованию национального стандарта конфиденциальности и способности последовательно сбалансировать риск конфиденциальности и ожидаемые выгоды при принятии решений и формулировании политики.

VII.8. Вызовы и барьеры, возникшие при принятии и внедрении систем.

Принятие и внедрение систем кибербезопасности и конфиденциальности может быть сопряжено с различными вызовами и барьерами. Ниже представлены некоторые из них:

- ***Отсутствие осведомленности и понимания:*** одной из существенных проблем является недостаточная осведомленность и непонимание сути систем и их преимуществ. Организации могут не до конца понимать требования и задачи системы, а также то, как они согласуются с их бизнес-целями.

- ***Ограниченность ресурсов:*** внедрение надежной системы обеспечения кибербезопасности и конфиденциальности требует выделения ресурсов, как в виде персонала, так и в виде финансовых вложений. Организации могут столкнуться с проблемой выделения достаточных ресурсов для обучения персонала, приобретения необходимых инструментов и технологий, проведения оценок, а также организации процессов текущего мониторинга и сопровождения.
- ***Сложная нормативно-правовая база:*** организации, работающие в разных юрисдикциях, могут столкнуться с трудностями при работе с сложной и развивающейся нормативно-правовой базой. В зависимости от отрасли и географического положения организации могут быть вынуждены соблюдать требования нескольких систем, стандартов и нормативных актов, что может привести к путанице и возникновению проблем с соблюдением требований.
- ***Организационная культура и сопротивление:*** внедрение систем обеспечения кибербезопасности и конфиденциальности часто требует значительных изменений в организационной культуре и сознании. Сопротивление сотрудников, отсутствие поддержки со стороны руководства, а также сопротивление внедрению новых процессов и технологий могут препятствовать успешному внедрению.
- ***Постоянные обновления и изменения:*** системы обеспечения кибербезопасности и конфиденциальности постоянно совершенствуются с учетом возникающих угроз и технологических достижений. Следить за этими изменениями и обеспечивать постоянное соответствие требованиям может быть непросто для организаций, особенно для тех, которые не обладают достаточным опытом в области кибербезопасности.

Важно отметить, что перечисленные вызовы не являются исчерпывающими, и организации могут столкнуться с дополнительными препятствиями, обусловленными их спецификой.

VII.9. Будущие тенденции и новые системы

VII.9.1 Новые тенденции и разработки в области кибербезопасности и конфиденциальности.

Изучение новых тенденций и разработок в области кибербезопасности и конфиденциальности очень важно для того, чтобы опережать развивающиеся угрозы и понимать прогресс в технологиях и практиках. Ниже представлены некоторые значимые тенденции и изменения:

- ***Искусственный интеллект и машинное обучение в кибербезопасности:*** Технологии искусственного интеллекта и машинного обучения все чаще используются в сфере кибербезопасности для анализа огромных массивов данных, обнаружения аномалий, выявления закономерностей и потенциальных угроз. Они позволяют повысить эффективность обнаружения угроз, автоматизировать процессы обеспечения безопасности и создать механизмы проактивной защиты.

- ***Безопасность Интернета вещей:*** в связи с быстрым ростом числа устройств Интернета вещей обеспечение безопасности и конфиденциальности взаимосвязанных устройств стало критически важным. Основное внимание уделяется внедрению надежных мер безопасности, включая строгую аутентификацию, безопасные обновления по беспроводной сети, шифрование и управление уязвимостями, для защиты устройств Интернета вещей и обрабатываемых ими данных.
- ***Безопасность облачных вычислений:*** по мере того как организации все активнее используют облачные сервисы, обеспечение безопасности и конфиденциальности данных, хранящихся и обрабатываемых в облаке, приобретает первостепенное значение. Технологии обеспечения безопасности облачных вычислений, такие как безопасное многопользовательское использование, шифрование, контроль доступа и анализ угроз, постоянно совершенствуются для устранения возникающих угроз и уязвимостей.
- ***Технологии повышения конфиденциальности:*** в связи с растущей обеспокоенностью по поводу конфиденциальности данных наблюдается рост разработки и внедрения технологий, повышающих уровень конфиденциальности. Эти технологии, включая криптографические методы, анонимизацию и дифференциальную конфиденциальность, направлены на защиту конфиденциальной информации, обеспечивая при этом анализ и обмен данными.
- ***Архитектура нулевого доверия (англ. Zero Trust Architecture):*** Zero Trust – это подход к кибербезопасности, который ставит под сомнение традиционную модель «доверяй, но проверяй». Он ориентирован на проверку каждого запроса на доступ, недоверие к чему-либо или кому-либо по умолчанию, независимо от их местонахождения, а также на строгий контроль доступа и непрерывный мониторинг всей сети.

Важно отметить, что сфера кибербезопасности и конфиденциальности очень динамична, и возникающие тенденции и изменения могут меняться с течением времени. Регулярное чтение авторитетных отраслевых отчетов, исследовательских работ, а также участие в конференциях и семинарах позволяет получить самую свежую информацию о новых тенденциях и изменениях.

VII.9.2 Ознакомление с другими или готовящимися выпуску системами обеспечения кибербезопасности и конфиденциальности, которые могут оказать влияние на цифровую среду.

Ряд других или готовящихся к выпуску систем обеспечения кибербезопасности и конфиденциальности могут оказать существенное влияние на цифровую среду. Ниже представлено несколько ярких примеров:

- ***Сертификация модели зрелости кибербезопасности (англ. Cybersecurity Maturity Model Certification):*** — это система, введенная Министерством обороны США для повышения уровня кибербезопасности организаций, входящих в оборонно-промышленный комплекс. От подрядчиков требуется соблюдения определенных уровней кибербезопасности и практики защиты конфиденциальной информации и систем.

- ***Закон Калифорнии о защите персональных данных потребителей (англ. California Consumer Privacy Act) и Закон Калифорнии о правах на неприкосновенность частной жизни (англ. California Privacy Rights Act):*** представляют собой законодательные акты о защите персональных данных, принятые в Калифорнии с целью защиты персональной информации потребителей и предоставления им контроля над ее сбором и использованием предприятиями. Эти законы устанавливают строгие требования к защите данных, включая обязательства по раскрытию информации, права потребителей и повышенные штрафы за несоблюдение требований.
- ***Общий регламент защиты персональных данных (англ. GDPR):*** это всеобъемлющее положение о конфиденциальности, введенное Европейским союзом (ЕС) с целью укрепления прав на защиту данных и регулирования обработки персональных данных. Регламент распространяется на организации по всему миру, работающие с данными граждан ЕС, и налагает обязательства, связанные с согласием, уведомлениями о нарушении данных, правами субъектов данных и подотчетностью.
- ***ISO/IEC 27701:2019:*** это международный стандарт, содержащий рекомендации по внедрению системы управления конфиденциальной информацией (англ. Privacy Information Management System). Стандарт помогает организациям создавать, поддерживать и постоянно совершенствовать систему управления конфиденциальной информацией (англ. Privacy Information Management System), соответствующую требованиям стандарта ISO/IEC 27001, и при этом решать проблемы конфиденциальности.
- ***Система кибербезопасности НИСТ 2.0 (англ. NIST Cybersecurity Framework 2.0):*** НИСТ выпустил проект системы кибербезопасности 2.0, который будет опубликован в начале 2024 года. Данный проект представляет собой существенное обновление системы кибербезопасности, впервые выпущенной в 2014 году с целью помочь организациям снизить риск кибербезопасности. Проект отражает изменения в сфере кибербезопасности и облегчает применение системы кибербезопасности на практике для всех организаций. Проект системы кибербезопасности 2.0 отражает ряд существенных изменений, включая расширение области применения, добавление шестой функции, «управление», а также улучшенное и расширенное руководство по внедрению системы кибербезопасности, особенно по созданию профилей. НИСТ также выпускает отдельный проект примеров реализации, включенных в проект ядра системы кибербезопасности 2.0 (англ. CSF 2.0 Draft Core), для публичного обсуждения. Эти примеры реализации призваны помочь организациям, особенно небольшим, эффективно использовать систему. НИСТ также анонсировал выпуск Справочного руководства системы кибербезопасности 2.0 (англ. Cybersecurity Framework 2.0 Reference Tool) – это новый ресурс, официально представленный НИСТ 15 августа 2023 года. Этот инструмент позволяет пользователям изучить проект Ядра системы кибербезопасности 2.0 (функции, категории, подкатегории, примеры реализации) и предлагает человеко- и машиночитаемые версии проекта ядра (в форматах JSON и Excel). В настоящее время инструмент позволяет пользователям просматривать и экспортировать фрагменты ядра системы, используя ключевые поисковые запросы. В конечном итоге этот инструмент позволит пользователям создавать собственную версию Ядра системы кибербезопасности 2.0 с

выбранными информационными ссылками и обеспечит простой и упорядоченный способ изучения различных аспектов Ядра системы кибербезопасности.

Вышеописанные системы отражают растущее внимание к вопросам кибербезопасности и конфиденциальности в различных отраслях и юрисдикциях. Организациям, которые работают в рамках этих систем или подпадают под действие соответствующих нормативных актов, необходимо понимать и выполнять их требования по защите данных и соблюдению нормативных требований.

VII.10. Заключение

В данном документе рассматривается важность кибербезопасности и конфиденциальности в современном цифровом мире, а также то, как система кибербезопасности и конфиденциальности может помочь организациям и странам защитить свои цифровые активы и информацию. В документе также приводится справочная информация о концепции кибербезопасности и конфиденциальности, в том числе о вызовах и угрозах, возникающих в этой области, а также о необходимости разработки систем, которыми должны руководствоваться организации в своей работе по защите от этих угроз.

Далее в документе приводится обзор систем кибербезопасности и обеспечения конфиденциальности, включая подробное описание системы кибербезопасности НИСТ (англ. НИСТ Cybersecurity Framework), ISO 27001, системы обеспечения конфиденциальности НИСТ (англ. НИСТ Privacy Framework) и ISO 29100. Эти системы содержат рекомендации и лучшие практики, которым должны следовать организации для повышения уровня кибербезопасности и обеспечения конфиденциальности.

Далее следует сравнение различных систем и представление конкретных примеров организаций, которые успешно их внедрили. Эти примеры включают такие компании, как Cisco Systems, Microsoft и округ Арлингтон, штат Вирджиния. В документе также описываются вызовы и барьеры, с которыми сталкиваются организации при принятии и внедрении этих систем.

Наконец, в данной документе рассматриваются будущие тенденции и новые системы в области кибербезопасности и конфиденциальности. В том числе рассматриваются другие или готовящиеся к выпуску системы, которые могут оказать влияние на цифровою среду.
Ниже представлены несколько важных выводов из отчета, подчеркивающих, почему каждой организации необходимо внедрить систему кибербезопасности и обеспечения конфиденциальности:

- ***Важность кибербезопасности и конфиденциальности:*** в связи с растущим использованием технологий и увеличением объема конфиденциальной информации, хранимой и передаваемой в цифровом виде, организациям и странам необходимо принимать надежные меры по защите своих цифровых активов и информации.

- ***Функции систем кибербезопасности и конфиденциальности:*** системы кибербезопасности и конфиденциальности могут помочь организациям и странам защитить свои цифровые активы и информацию. В них содержатся практические рекомендации и лучшие практики, которым могут следовать организации для повышения уровня кибербезопасности и конфиденциальности.
- ***Широко известные системы кибербезопасности и конфиденциальности:*** системы кибербезопасности и конфиденциальности, включая систему кибербезопасности НИСТ, ISO 27001, систему обеспечения конфиденциальности НИСТ и ISO 29100, содержат подробное руководство и примеры для организаций по улучшению кибербезопасности и защиты конфиденциальности. Для организаций было бы хорошей инициативой рассмотреть возможность внедрения этих систем на основе уже имеющихся примеров использования.
- ***Проблемы и барьеры на пути внедрения:*** существует ряд проблем и препятствий, с которыми сталкиваются организации при принятии и внедрении этих систем. К ним относятся такие факторы, как недостаток понимания, ограниченность ресурсов, сложная нормативная база, организационная культура и сопротивление изменениям.
- ***Принятие подходящих систем для обеспечения готовности:*** с появлением новых систем кибербезопасности и конфиденциальности лучше понять, какие системы подходят для каждой организации, чтобы рассмотреть возможность их принятия и внедрения в своей организации для подготовки к постоянно меняющимся условиям и рискам.

Системы кибербезопасности и конфиденциальности не являются панацей. Они являются эффективными инструментами, которые могут помочь организациям повысить уровень безопасности и конфиденциальности, но не гарантируют идеальных решений. Организациям необходимо постоянно отслеживать ситуацию и адаптировать свои меры по обеспечению готовности по мере развития угроз и тенденций в области регулирования.

Защита кибербезопасности и конфиденциальности - обязанность каждого. Один человек или один отдел не может отвечать за защиту информационных активов и персональных данных организации. Системы кибербезопасности и конфиденциальности помогают обеспечить осознание всеми сотрудниками организации своей роли в защите данных и систем.

Однако системы кибербезопасности и конфиденциальности должны соответствовать конкретным потребностям организации. Не существует универсального подхода по вопросу обеспечению кибербезопасности или конфиденциальности. Выбор оптимальной системы для организации зависит от ее масштаба, отрасли и степени риска.

Внедрение системы кибербезопасности и конфиденциальности – это постоянный процесс. Это не то, что можно сделать один раз и забыть об этом. Организациям необходимо регулярно пересматривать и обновлять свои меры безопасности и защиты, чтобы не отставать от угроз.

Наконец, кибербезопасность и конфиденциальность – это инвестиции, а не расходы. Затраты на внедрение и поддержку систем кибербезопасности и конфиденциальности могут быть значительными, но цена нарушения конфиденциальности данных может быть гораздо выше. Инвестируя в кибербезопасность и конфиденциальность, организации могут обезопасить свои данные, свою репутацию и свою прибыль.

ОБСУЖДЕНИЕ

В данной публикации основное внимание уделено стандартам и лучшим международным практикам, которые считаются ключевыми для преодоления сложностей цифровой эпохи и развития цифровой трансформации. Она представляет собой всеобъемлющий обзор признанных международных стандартов, подчеркивающий стремление к созданию лучших практик, обеспечению безопасности данных и повышению эффективности государственных услуг.

Настоящий документ также отражает уникальные потребности и интересы стран-участниц регионального проекта по наращиванию потенциала и их приверженность к решению потребностей с помощью единого ресурса. Ожидается, что данный документ послужит практическим руководством по применению этих стандартов в различных областях цифровизации, повышая тем самым эффективность, безопасность и результативность работы государственных органов.

Выбор авторитетных международных стандартов, включая Библиотеку инфраструктуры информационных технологий (англ. Information Technology Infrastructure Library), Архитектуру взаимодействия электронного правительства (англ. e-Government Interoperability Framework), Методику описания архитектуры, разработанную Open Group (англ. TOGAF), Задачи управления для информационных и смежных технологий (англ. COBIT), Эталонную архитектуру облачных вычислений (англ. Cloud Computing Reference Architecture Framework), Общий регламент защиты персональных данных (англ. GDPR), ISO/IEC 27001 и систему кибербезопасности (англ. Cybersecurity Framework), отражает комплексный подход к решению различных аспектов цифровой трансформации. В совокупности эти системы формируют надежный фундамент для правительств и организаций на их пути к цифровым технологиям, обеспечивая целостность и безопасность их цифровых инициатив, что в конечном итоге приносит пользу гражданам и заинтересованным сторонам.

Внедрение Библиотеки инфраструктуры информационных технологий (англ. Information Technology Infrastructure Library, ITIL) в государственных организациях способно изменить систему предоставления государственных услуг, переняв успехи частного сектора. ITIL ставит во главу угла совершенствование услуг, ориентированное на граждан, и адаптирует государственные услуги к потребностям населения. Такая ориентация на качество услуг способствует укреплению доверия, создавая впечатление надежности и оперативности работы правительства. Циклический подход ITIL соотносит ИТ-стратегии с более широкими общественными интересами, повышая эффективность работы государственных органов. ITIL снижает риски, сводя к минимуму перебои в предоставлении услуг, что очень важно в государственных органах, где перебои могут иметь серьезные последствия. ITIL оптимизирует операции, устраняет избыточность и оптимизирует распределение ресурсов, что приводит к экономически эффективному предоставлению государственных услуг. Поощряется межведомственное взаимодействие, что способствует командной работе и обмену знаниями, позволяя находить комплексные решения сложных задач. Четкое документирование способствует прозрачности и подотчетности, а итерационный характер ITIL позволяет ведомствам адаптироваться к изменяющимся условиям. В конечном итоге ITIL оптимизирует

использование ресурсов, обеспечивая более высокую эффективность и способствуя развитию сотрудничества и подотчетности между заинтересованными сторонами. Таким образом, внедрение ITIL в государственном управлении приводит к созданию ориентированной на граждан, эффективной и подотчетной системы предоставления государственных услуг, повышающей качество обслуживания и отвечающей общественным интересам.

В свою очередь, Архитектура взаимодействия электронного правительства (англ. e-Government Interoperability Framework, e-GIF) устанавливает техническую политику и спецификации для достижения совместимости и согласованности систем ИКТ в многочисленных государственных организациях, определяя основные предпосылки для объединенного правительства с поддержкой веб-технологий. Это технический краеугольный камень совместимости цифровых систем государственного сектора, позволяющий предоставлять современные и более совершенные государственные услуги. Данная система определяет минимальный набор технических политик и спецификаций, регулирующих информационные потоки между государственными организациями в отношении взаимосвязи, интеграции данных, метаданных управления контентом и доступа к электронным услугам.

Интеграция Методики описания архитектуры, разработанной Open Group (англ. TOGAF), в деятельность государственного сектора предлагает структурированный и очень выгодный подход к управлению ИТ-системами. Он ориентирован на эффективное распределение ресурсов, выявление возможностей экономии и минимизацию потерь. Ключевым преимуществом является акцент на стандартизации и совместимости, что позволяет государственным органам работать слаженно и сократить дублирование усилий. Кроме того, TOGAF играет важную роль в повышении уровня безопасности и соответствия ИТ-систем государственных органов, противодействуя растущим угрозам кибербезопасности и нормативным требованиям. TOGAF предлагает системы для безопасной ИТ-архитектуры, защиты конфиденциальных государственных данных и обеспечения соответствия нормативным требованиям. Кроме того, TOGAF позволяет сократить расходы и оптимизировать ресурсы за счет анализа существующих ИТ-ресурсов, устранения избыточности и оптимизации операций. Это не только экономит расходы, но и обеспечивает направление ресурсов туда, где они наиболее необходимы. В эпоху бюджетных ограничений TOGAF предоставляет государственным организациям эффективный инструмент для эффективной и ответственной работы в условиях постоянно меняющегося технологического ландшафта.

Задачи управления для информационных и смежных технологий (англ. COBIT) – это признанная система, имеющая огромное значение для государственных организаций. Она обеспечивает соответствие ИТ-стратегий государственных органов более широким государственным задачам, что позволяет эффективно использовать инвестиции в технологии в интересах общества. COBIT предлагает комплексную систему управления, которая необходима для контроля ИТ-операций в государственных органах, обеспечивая эффективность и соблюдение государственных интересов. В условиях государственного управления, когда на карту поставлены конфиденциальные данные и критически важные услуги, возможности COBIT по управлению рисками приобретают первостепенное значение. COBIT позволяет выявлять и снижать риски, защищая данные и обеспечивая

непрерывность работы основных услуг. Еще одним важным аспектом для государственных органов является соответствие нормативным требованиям, и COBIT представляет четкие рекомендации по соблюдению этих стандартов, снижая риск возникновения правовых проблем и штрафов. Функции COBIT по оптимизации ресурсов помогают государственным органам выявлять неэффективные процессы, сокращать избыточность и экономически эффективно распределять ресурсы, способствуя принятию взвешенных решений. Взаимодействие и стандартизация также способствуют улучшению координации между государственными органами и повышению эффективности предоставления государственных услуг. Основные характеристики и преимущества COBIT способствуют повышению эффективности управления, управления рисками, оптимизации ресурсов и соблюдения нормативных требований в государственных ИТ-системах. Внедрение COBIT позволяет государственным органам эффективно управлять ИТ-процессами, согласовывать их с государственными целями, снижать риски, обеспечивать соответствие нормативным требованиям и, в конечном счете, предоставлять более прозрачные и эффективные государственные услуги.

Внедрение Эталонной архитектуры облачных вычислений (англ. Cloud Computing Reference Architecture Framework), в государственных организациях дает ряд существенных преимуществ. Эталонная архитектура позволяет оптимизировать использование ресурсов, снизить затраты и обеспечить бюджетную эффективность. Масштабируемость позволяет государственным органам быстро адаптироваться к изменяющимся требованиям, а возможности быстрого развертывания - оперативно реагировать на изменяющиеся требования. Функциональная совместимость обеспечивает бесперебойное взаимодействие между государственными органами, сохраняя безопасность данных. Соблюдение стандартов безопасности и соответствия нормативным требованиям обеспечивает защиту конфиденциальных данных в эпоху растущих киберугроз. Эффективное управление данными обеспечивает их качество и доступность, позволяя принимать решения на основе данных. Оптимизация ресурсов, снижение затрат на обслуживание ИТ и межведомственное взаимодействие способствуют повышению эффективности и инновационности. Архитектура согласует облачные инициативы с более широкими государственными задачами, позволяя государственным органам лучше оказывать услуги гражданам и выполнять свою миссию, соблюдая при этом нормативные требования. По сути, внедрение эталонной архитектуры облачных вычислений в государственных структурах повышает эффективность, безопасность и рентабельность, модернизируя и оптимизируя ИТ-системы для удовлетворения меняющихся общественных потребностей.
Принятие Общего регламента защиты персональных данных (англ. GDPR), в государственных органах имеет ряд существенных преимуществ. GDPR подчеркивает важность защиты данных и конфиденциальности, что очень важно для государственных организаций, работающих с огромными объемами персональных и конфиденциальных данных, и тем самым повышает доверие граждан. Соблюдая GDPR, государственные органы могут упростить сложную законодательную базу в области защите данных, обеспечивая соблюдение правовых норм, особенно при работе с гражданами или организациями Европейского союза. GDPR также способствует повышению подотчетности и прозрачности, позволяя государственным органам быть более прозрачными в отношении своей работы с данными. Особое внимание уделяется безопасности данных, что является важным аспектом, учитывая растущую угрозу утечки

данных и кибератак. Укрепляются права граждан на их персональные данные, что расширяет их возможности и усиливает контроль. Кроме того, GDPR требует своевременного информирования об утечках данных, что побуждает государственные органы совершенствовать механизмы реагирования. Оценка воздействия на защиту данных способствует проактивному управлению рисками, а соблюдение требований GDPR упрощает процессы международной передачи данных. Поощряя минимизацию данных и ограничение целей, GDPR помогает государственным учреждениям избежать чрезмерного сбора данных и обеспечить соответствие требованиям конфиденциальности. Кроме того, GDPR предлагает систему для обучения и повышения осведомленности сотрудников, способствуя формированию культуры конфиденциальности в государственных организациях. Принципы согласия, соглашения об обработке данных и назначение сотрудников по защите данных обеспечивают структурированный подход к работе с персональными данными. Кроме того, GDPR способствует развитию трансграничного сотрудничества между органами по защите данных. Более того, его глобальное влияние привело к принятию аналогичных принципов защиты данных и конфиденциальности во всем мире. Правительства стран, не входящих в ЕС, могут увидеть преимущества в гармонизации с требованиями GDPR для обеспечения последовательности и международной передачи данных. По сути, внедрение принципов GDPR в государственном управлении способствует повышению уровня защиты данных, соблюдению правовых норм, прозрачности и подотчетности. Это способствует укреплению общественного доверия и расширению прав и возможностей граждан, а также обеспечивает проактивность государственных органов в решении проблем защиты данных и конфиденциальности, адаптируясь к их конкретным потребностям и нормативной базе.

Принятие стандарта ISO/IEC 27001:2022 в государственных организациях предлагает структурированную и признанную на международном уровне систему для управления информационной безопасностью. Такой подход обеспечивает ряд ключевых преимуществ, включая повышение уровня информационной безопасности, соответствие законодательным и нормативным требованиям, эффективное управление рисками и усиление защиты данных. Кроме того, стандарт способствует повышению операционную безопасность, облегчает межведомственное взаимодействие и укрепляет общественное доверие благодаря надежным методам защиты данных. Распределение ресурсов становится более экономичным, а отношения с третьими сторонами - более надежными. Международное признание стандарта облегчает соответствие лучшим международным практикам, а реагирование на инциденты, управление данными и регулярные аудиты обеспечивают проактивный и эволюционирующий (находящийся в постоянном развитии) подход к безопасности. Программы обучения и повышения осведомленности позволяют государственным служащим понимать и соблюдать стандарты информационной безопасности. По сути, принятие стандарта ISO/IEC 27001:2022 дает возможность государственным органам повысить уровень своей информационной безопасности, способствуя укреплению общественного доверия и надежному реагированию на риски. Однако его эффективность зависит от приверженности государственных органов поддержанию высоких стандартов информационной безопасности.

Внедрение в государственных организациях системы кибербезопасности НИСТ (англ. НИСТ Cybersecurity Framework) представляет собой структурированный и признанный на

международном уровне подход к повышению уровня кибербезопасности. Преимущества такого подхода многочисленны, включая повышение уровня кибербезопасности, эффективное управление рисками и соответствие законодательным и нормативным требованиям. Кроме того, система способствуют функциональной совместимости и сотрудничеству, укрепляют защиту данных и обеспечивают эффективное реагирование на инциденты. Кроме того, системы кибербезопасности обеспечивают безопасность цепочек поставок, оптимизируют распределение ресурсов и повышают доверие населения к государственным органам. Они способствуют взаимодействию с частным сектором, международному сотрудничеству и глобальному влиянию на установление стандартов кибербезопасности. Обучение и подготовка персонала, обмен информацией об инцидентах, меры по аудиту и подотчетности способствуют созданию целостной и надежной среды кибербезопасности. По сути, принятие системы кибербезопасности (англ. Cybersecurity Framework) позволяет государственным органам работать в сложной и меняющейся ситуации, связанной с киберугрозами при условии, что гос. органы обязуются эффективно внедрять и поддерживать высокий уровень кибербезопасности в своих учреждениях.

Исследовательская группа Астанинского хаб государственной службы в сотрудничестве с экспертами Национального агентства по развитию информационного общества Республики Корея рассчитывает, что данный информационный продукт позволит значительно повысить уровень цифровизации деятельности государственных органов и улучшить предоставление государственных услуг. Обмениваясь ценной информацией и продвигая самые высокие стандарты цифровой трансформации, он внесет существенный вклад в постоянный прогресс и успех стран-участниц в условиях постоянно меняющейся цифровой среды.

Аббревиатуры и сокращения

ACSH	Астанинский хаб государственной службы
ADM	Метод разработки архитектуры
ИИ	Искусственный интеллект
API	Интерфейс прикладного программирования
APO	Координация, планирование и организация
ПЭМ	Прикладная эталонная модель
BAI	Разработка, приобретение и внедрение
BGP	Протокол пограничного шлюза
BRM	Эталонная бизнес-модель
ССП	Сбалансированная система показателей
CA	Центр сертификации
ХБРЯ	Химическое, биологическое. Радиологическое, ядерное
CCPA	Закон Калифорнии о защите персональных данных потребителей
CCRA	Эталонная архитектура облачных вычислений
CCTA	Центральное агентство по вычислительной технике и телекоммуникациям
CD	Непрерывное развёртывание
CDN	Сеть доставки контента
CEO	Руководитель, Генеральный директор
CERT	Служба реагирования на компьютерные инциденты
CGSI	Индекс базовой государственной системы
CI	Непрерывная интеграция
CIO	Директор по информационным технологиям
COBIT	Задачи управления для информационных и смежных технологий
CMMC	Сертификация модели зрелости кибербезопасности
CMMI	Интеграция моделей зрелости возможностей
CNIL	Национальная комиссия по вопросам информационных прав и свобод
CNPD	Национальная комиссия по защите данных
CPM	Цена за тысячу показов
CQRS	Разделение ответственности на команды и запросы
CRM	Консолидированная эталонная модель, управление взаимоотношениями с клиентами
CSF	Система кибербезопасности
CSI	Постоянное совершенствование услуг
БД	База данных
DCEI	Индекс вовлеченности граждан в цифровую среду
DDoS	Распределенный отказ в обслуживании
DGI	Индекс развития электронного правительства
DGA	Закон об управлении данными
DMV	Департамент транспортных средств
DNA	Данные, сеть и искусственный интеллект
DNS	Система имен доменов
DPA	Агентство по защите данных
DPIA	Оценка воздействия на защиту данных
DPO	Сотрудник по защите данных

МО	Министерство обороны
DODAF	Методика описания архитектуры Министерства обороны США
DRM	Эталонная модель данных
DSK	Независимый орган по защите данных Германии
DSM	Единый цифровой рынок
DSS	Предоставление, обслуживание и поддержка
EA	Архитектура предприятия [схема]
EAMS	Служба управления корпоративным доступом
ТС	Европейское сообщество
ECCP	Европейский центр сертификации
EDPB	Европейский совет по защите данных
EGDI	Индекс развития электронного правительства
e-GIF	Архитектура взаимодействия электронного правительства
EGIT	Корпоративное управление информационными технологиями
e-GMS	Стандарт метаданных электронного правительства
EIF	Европейская структура совместимости
ЕС	Европейский союз
ЧЗД	Часто задаваемые вопросы
FDS	Федеральная стратегия управления данными
FEA[F]	Федеральная архитектура государственных организаций США
FedRAMP	Федеральная программа управления рисками и авторизацией
GCL	Список правительственных категорий
GDPR	Общий регламент защиты персональных данных
GDS	Стандарты государственных данных
GDSC	Каталог стандартов государственных данных
GEAP	Процесс создания архитектуры государственного предприятия
GSI	Защищенная правительственная внутренняя сеть
GTEI	Индекс институциональной среды GovTech
GTMI	Индекс зрелости GovTech
JSON	Открытый стандарт представления данных, основанный на JavaScript
УТР	Управление трудовыми ресурсами
HTTP	Протокол передачи гипертекста
IaaS	Инфраструктура как услуга
ИКТ	Информационные и коммуникационные технологии
ИСР	Интегрированная среда разработки
МЭК	Международная электротехническая комиссия
IoT	Интернет вещей
IP	Межсетевой протокол
IRM	Эталонная модель инфраструктуры
ISACA	Международная профессиональная ассоциация ИТ
ISO	Международная организация по стандартизации
СУИБ	Система менеджмента информационной безопасности
ITSM	Система управления ИТ услугами
ИТ	Информационные технологии
ITIL	Библиотека инфраструктуры информационных технологий
KEPCO	Корейская электроэнергетическая корпорация
КПЭ	Ключевые показатели эффективности

KRW	Южнокорейская вона
LAN	Локальная вычислительная сеть
MEA	Мониторинг, оценка и анализ
ВО	Военная операция
MIT	Массачусетский технологический институт
ML	Машинное обучение
МВДиБ	Министерство внутренних дел и безопасности (Республика Корея)
NAC	Контроль доступа к сети
НАТО	Организация Североатлантического договора
NDS	Национальная стратегия в области данных
NIA	Национальное агентство по развитию информационного общества (Республики Корея)
NIEM	Национальная модель обмена информацией
NIF	Национальная система обеспечения функциональной совместимости
NIIS	Институт решений по взаимодействию стран Северной Европы
НИСТ	Национальный институт стандартов и технологий
NTIS	Национальная служба научно-технической информации
ОЭСР	Организация экономического сотрудничества и развития
OGC	Управление государственной торговли
OMB	Административно-бюджетное управление
ОС	Операционная система
PaaS	Платформа как услуга
PCI DSS	Стандарт безопасности данных индустрии платежных карт
PDCA	Цикл планирование-действие-проверка-корректировка
PET	Технологии повышения конфиденциальности
ПИИ	Персональная идентификационная информация
PRM	Эталонная модель производительности
PSDI	Индекс предоставления государственных услуг
REST	Передача состояния представления
RFC	Протокол запроса комментариев
SaaS	Программное обеспечение как услуга
ЦУР	Цели устойчивого развития
SDM	Стандартная модель защиты данных
SIB	Информационная база стандартов
SLA	Соглашение об уровне предоставления услуги
МСБ	Малый и средний бизнес
SMIME	Защищенные многоцелевые интернет-почтовые расширения
SMTP	Простой протокол передачи почты
SoA	Положение о применимости
SOAP	Простой протокол доступа к объектам
SRM	Эталонная модель услуг
Протокол SSL	Протокол безопасности, создающий зашифрованное соединение между веб-сервером и веб-браузером
ППО	Прикладное программное обеспечение
TAFIM	Базовая архитектура технического обеспечения для управления информацией

Протокол TCP	Протокол управления передачей
TEAF	Методика описания архитектуры казначейства США
TOGAF	Методика описания архитектуры разработанная Open Group
TRM	Эталонная модель технологии
Протокол TLS	Протокол шифрования соединения между двумя серверами, обеспечивающий защищенную передачу данных между узлами сети Интернет
TSA	Служба штампов времени
TSC	Каталог технических стандартов
ОАЭ	Объединенные Арабские Эмираты
ООН	Организация Объединенных Наций
ПРООН	Программа развития Организации Объединенных Наций
ЮНИДО	Организация Объединенных Наций по промышленному развитию
URL	Унифицированный указатель ресурса
США	Соединенные Штаты Америки
USB	Универсальная последовательная шина
VM	Виртуальная машина
VPC	Виртуальное частное облако
VPN	Виртуальная частная сеть
ВБ	Всемирный банк
WWW	Всемирная паутина
Язык-XML	Расширяемый язык разметки

Программа развития ООН
Площадь Организации
Объединенных Наций
Нью-Йорк, 10017
www.undp.org

Астанинский хаб
государственной службы
Здание ООН
г. Астана, улица Мамбетова 14, Z11D8T7
www.astanacivilservicehub.org.