Исследование навыков кибербезопасности стандарта SFIA8

О.С. Белякова, В.А. Сухомлин

***Аннотация* — В условиях цифровизации большинства сфер человеческой деятельности проблема массовой подготовки ИТ-специалистов становится чрезвычайно важной. В связи с чем актуальной задачей представляется создание цифровой платформы, позволяющей организациям в режиме реального времени сообщать о своих потребностях в специалистах для заполнения вакансий на рабочих местах, а системе образования реагировать на соответствующие потребности работодателей и предлагать актуальные программы подготовки и переподготовки востребованных кадров. Примером такой платформы может служить платформа развития цифровых навыков, разработка которой ведется в рамках проектной деятельности лаборатории открытых информационных технологий факультета ВМК МГУ. В качестве методологической базы разрабатываемой платформы выбран стандарт цифровых навыков организации SFIA, представленный в виде одноименного фреймворка. В сентябре 2021 года вышла новая версия фреймворка – SFIA8, в которую по сравнению с предыдущей версией стандарта добавлены два десятка новых навыков и пересмотрена семантика ряда навыков предыдущей версии. Также характерной особенностью нового этапа развития подхода SFIA стала разработка на основе навыков SFIA кластеров ролей (так называемых взглядов SFIA), соответствующих актуальным технологическим сферам, таким, как, например, цифровая трансформация, большие данные, программная инженерия, кибербезопасность и др. В первой части статьи приводится анализ основных нововведений в стандарте SFIA8. Вторая часть посвящена исследованию семантики (знаний-умений) навыков SFIA8, прямо или косвенно относящихся к кибербезопасности. В процессе определения состава таких навыков в первую очередь рассматривались навыки, указанные во взгляде SFIA8 Информационной и кибербезопасности. Результаты исследования семантики навыков кибербезопасности размещены в приложении. Предложенное описание навыков кибербезопасности SFIA8 в разрезе знаний и умений в первую очередь ориентировано на методистов и преподавателей системы образования, разрабатывающих программы подготовки профессионалов в области кибербезопасности.**

***Ключевые слова* — кибербезопасность, информационная безопасность, цифровые навыки, платформа развития цифровых навыков, стандарт SFIA.**

I. Введение

Глобальный процесс цифровизации, охвативший по существу все сферы человеческой деятельности и бытия, включая промышленность, экономику, науку, культуру и образование определил как чрезвычайно важную проблему массовой подготовки людей с цифровыми навыками, необходимыми для активного участия в цифровой экономике. Поэтому задача создания образовательных технологий, направленных на выявление и развитие востребованных цифровых навыков, признана на Министерской конференции в Канкуне (Мексика), где была принята Декларация Министров «О цифровой экономике: инновации, рост и социальное благополучие», как глобальная и актуальная [1].

В связи с этим создание цифровой платформы, позволяющей организациям в режиме реального времени сообщать о своих потребностях в специалистах для заполнения вакансий на рабочих местах, а системе образования реагировать на соответствующие потребности работодателей и предлагать актуальные программы подготовки и переподготовки востребованных кадров, представляется своевременным и нужным решением. Примером такой платформы может являться платформа развития цифровых навыков, разработка которой ведется в рамках проектной деятельности лаборатории открытых информационных технологий факультета ВМК МГУ [2]. Такая платформа выполняет роль рабочей площадки для взаимодействия нескольких заинтересованных сторон, а именно, учебных заведений, организаций-работодателей, потенциальных учащихся [3].

Методической основой такой платформы должен служить признанный на международном уровне стандарт классификации и описания цифровых навыков, как обще используемый язык для определения функциональности рабочих ролей, требований к компетенции исполнителей ролей, их социально-личностным качествам. Наиболее известными и популярными системами классификации навыков/компетенций являются: e-CF [4], iCD [5], SFIA [6]. В сравнительном анализе этих систем, выполненным в работе [7], обоснован выбор в качестве базовой методологии для рассматриваемой выше платформы фреймворка SFIA. В сентябре 2021 года вышла новая версия фреймворка – SFIA8, в которую по сравнению с предыдущей версией стандарта добавлены порядка двух десятков новых навыков и пересмотрена семантика ряда навыков предыдущей версии. Также характерной особенностью нового этапа развития подхода SFIA стала разработка на основе навыков SFIA кластеров ролей (так называемых взглядов SFIA), соответствующих актуальным технологическим сферам, таким, как,

Статья получена 20 мая 2022.
О.С. Белякова – МГУ имени М.В. Ломоносова (e-mail: osbelyakova@yandex.ru).
В.А. Сухомлин – МГУ имени М.В. Ломоносова (e-mail: sukhomlin@mail.ru).

например, цифровая трансформация, большие данные, программная инженерия, кибербезопасность и др.

Все это привело к необходимости исследовать нововведения и другие изменения в стандарте SFIA, с тем чтобы учесть их при создании платформы развития цифровых навыков. Анализ этих изменений составляет первую часть статьи.

Вторая часть статьи посвящена исследованию семантики (знаний-умений) навыков SFIA8, прямо или косвенно относящихся к кибербезопасности. Для исследования выделены две группы навыков стандарта: в группу А* отнесены навыки, непосредственно связанные с кибербезопасностью, в группу Б* – те навыки, в рамках которых решаются отдельные задачи, связанные с информационной безопасностью. В процессе определения состава групп в первую очередь рассматривались навыки, указанные во взгляде Информационной и кибербезопасности фреймворка SFIA8 [8].

Результаты исследования семантики навыков кибербезопасности размещены в приложении. Предложенное описание навыков кибербезопасности SFIA8 в разрезе знаний и умений ориентировано на методистов и преподавателей системы образования, разрабатывающих программы подготовки профессионалов в области кибербезопасности.

II. Стандарт SIFA

Модель SFIA представляет собой наднациональный инструмент для описания и управления компетенциями специалистов в 21 веке. Система SFIA принадлежит и управляется Фондом SFIA — консорциумом, созданным в июле 2003 года Институтом инжиниринга и технологий (Institution of Engineering and Technology, IET), Институтом менеджмента информационных систем (Institute for the Management of Information Systems, IMIS), Центром электронных навыков Великобритании (e-skills UK) и Британским компьютерным обществом (British Computer Society , BCS) [7].

Фонд SFIA разработал и поэтапно развивает одноименный стандарт с общеупотребительными описаниями профессиональных навыков, необходимых работающим в области информационных технологий. Стандарт определяет набор согласованных уровней карьерного роста, вводит четкое различие профессиональных навыков и технических знаний. Стандарт отличается системностью, глобальным применением в различных странах и непрерывной поддержкой в части развития.

SFIA оперирует двумя основными категориями: навыками и уровнями ответственности.

В сентябре 2021 года вышла новая версия фреймворка SFIA8, позиционируемая создателями как новая версия глобальной системы навыков и компетенций цифрового мира.

В общей сложности 8-я версия SFIA содержит описание 121 навыка. Классификация навыков представляет собой трехуровневую иерархическую структуру: включающую категории, подкатегории и собственно сами навыки.

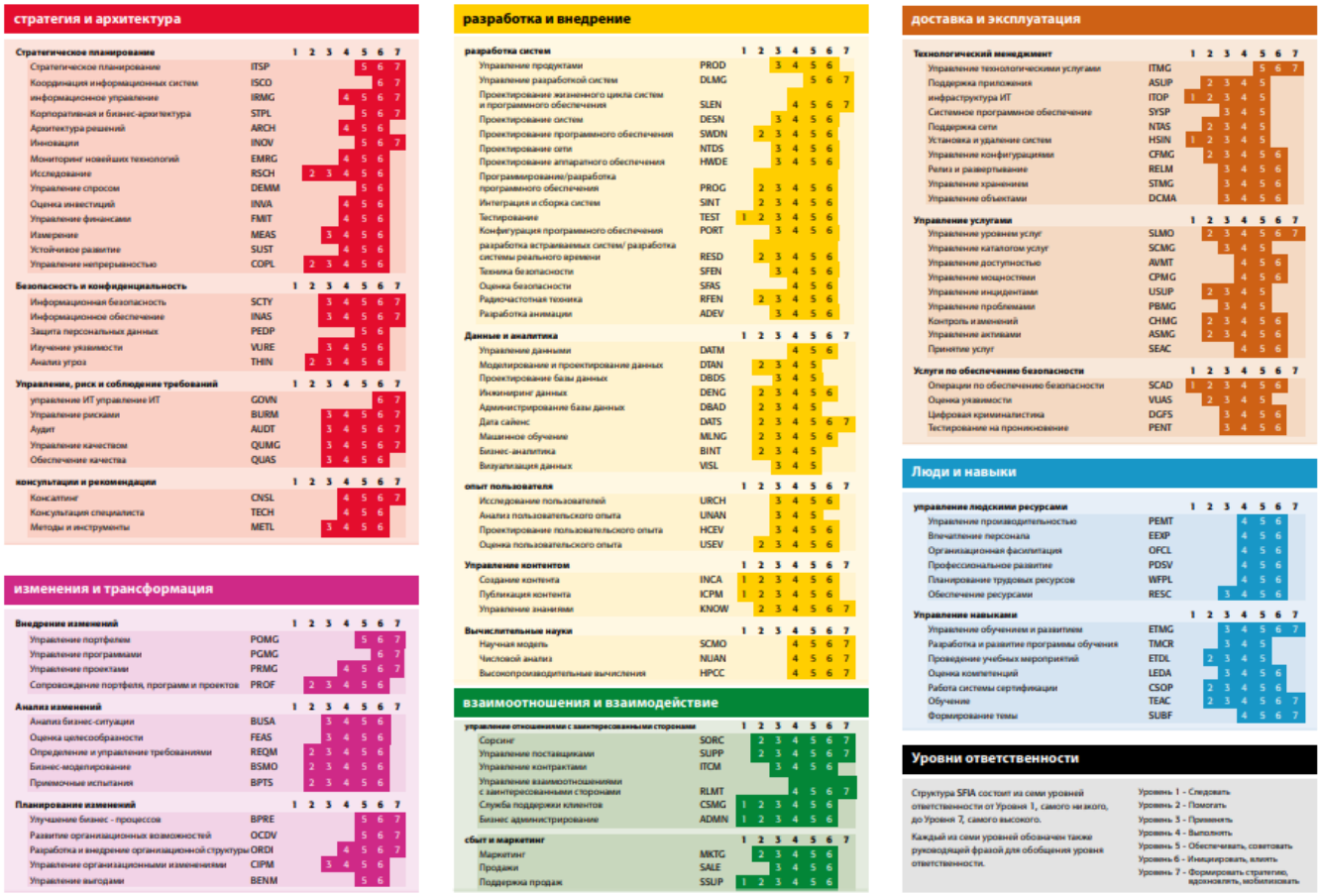

Рисунок 1. Сводная таблица категорий, подкатегорий, навыков SFIA8 [6].

Как продемонстрировано на рис.1, SFIA8 делит свои навыки на 6 категорий, которые в свою очередь содержат

в совокупности 19 подкатегорий навыков.

Для каждого навыка имеются свои доступные уровни ответственности. В SFIA вводится 7 таких уровней. Каждый уровень предполагает разные уровни автономии сотрудника, влияния на других сотрудников, сложности его деятельности и бизнес-навыков, которыми он должен обладать. Уровни описывают поведение, ценности, знания и характеристики, которыми должен обладать специалисты, чтобы быть признанными компетентными на конкретном уровне.

Уровни ответственности и, в частности, их общие характеристики (Автономность, Влияние, Сложность, Знания, Бизнес-навыки; Безопасность, Конфиденциальность и этика) используются вместе с навыками для описания компетенции.

Каждое описание навыка содержит общее определение навыка и описание навыка для тех из семи уровней, которые доступны для него (рис.2). Эти описания являются подробным определением того, что значит владеть навыком на соответствующем уровне ответственности.

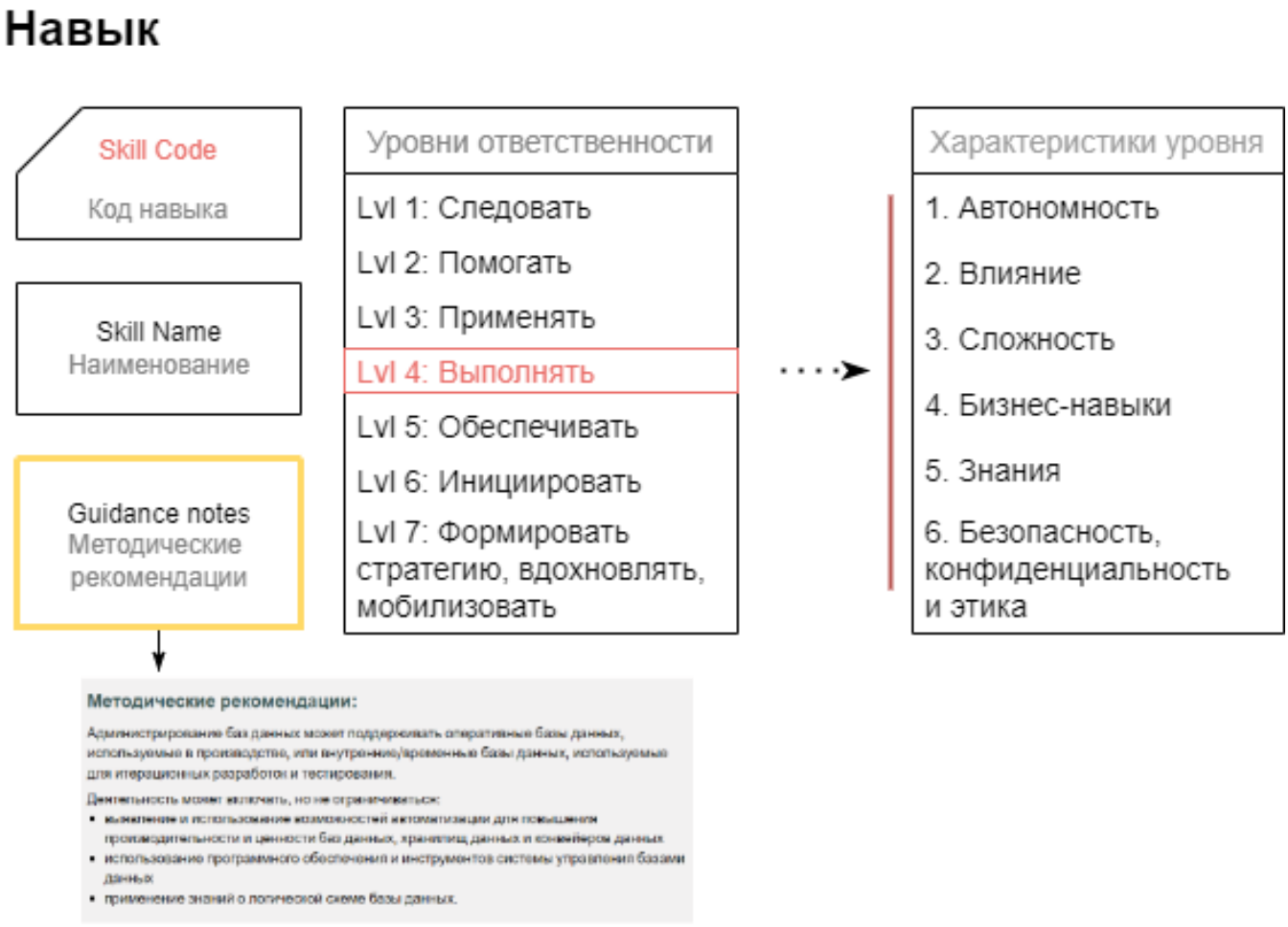

Рисунок 2. Структура навыка SFIA.

Система навыков SFIA по существу предлагает общую систему ценностей для оценки широкого профессиональных компетенций. Образовательные организации, университеты, колледжи и тренинговые центры сопоставляют свои предложения с моделью SFIA, чтобы предлагать актуальные учебные программы для развития требуемых навыков на требуемом уровне.

III. Обзор SIFA

Взгляды SFIA

SFIA 8 предлагает пользователям так называемые взгляды SFIA (SFIA view) – это группы навыков, соответствующие определенным профессиональным сферам деятельности. Например, взгляд для сферы Информационной и кибербезопасности состоит из 6-ти разделов навыков:

1. Навыки для специалистов по безопасности (Skills for security professionals).
2. Программы безопасности (Security programmes).
3. Обеспечение безопасной разработки программного обеспечения (Secure software development).
4. Обеспечение защищенности инфраструктуры (Secure infrastructure).
5. Управление практикой безопасности (Security practice management).
6. Другие навыки, связанные с безопасностью (Other security related skills).

Группы навыков этих разделов не пересекаются, и все навыки, так или иначе связанные с кибербезопасностью, охватываются взглядом.

Поведенческие факторы

Другой важной особенность SFIA8 становится появление поведенческих факторов как характеристик уровней ответственности. Разбиение каждого уровня ответственности на поведенческие факторы является полезным инструментом для поддержки жизненного

цикла управления навыками и соответствующей деятельности.

Перечень поведенческих факторов, конкретизирующих каждый из 7 уровней ответственности, соотносится с характеристиками уровней ответственности, как показано на рисунке ниже:

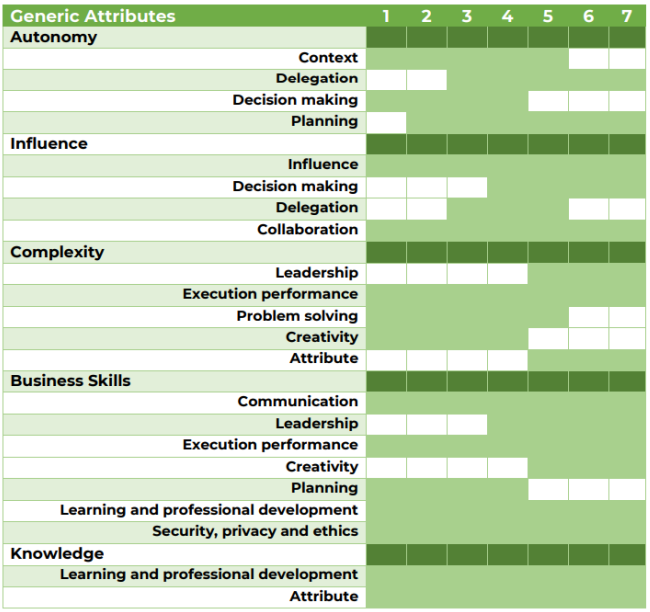

Рисунок 3. Расположение поведенческих факторов в характеристиках уровней ответственности [6].

В соответствии с принципами разработки SFIA, описания поведенческих факторов являются общими по содержанию для всех навыков стандарта SFIA, чтобы обеспечить их универсальное применение к структуре организации, системе возможностей и методам работы.

Изменение состава навыков

Рассмотрим количественные изменения в стандарте [6] и изменения содержания их описания, которые отразились в версии фреймворка SFIA8, акцентируя внимание на обновлении навыков области кибербезопасности [9].

Во-первых, в состав SFIA были добавлены 24 новых навыка. Раздел “Информационная и кибербезопасность” пополнился следующими навыками:

1. VURE: Исследование уязвимостей
2. VUAS: Оценка уязвимостей
3. THIN: Аналитика угроз

Далее, некоторые навыки были исключены из списка фреймворка.

Следующие навыки были пересмотрены и заменены:

- INAN: Аналитика (Analytics)
- BUAN: Бизнес-анализ (Business analysis)
- CORE: Проверка соответствия (Conformance review)
- NTPL: Планирование сети (Network planning)

При этом в целом с содержательной точки зрения охват описаний SFIA области ИТ естественно не уменьшился - на замену исключенным навыкам введены несколько новых или же модифицированных старых, которые покрывают содержание удаленных навыков.

Семь навыков SFIA были переименованы, в том числе 3 из них, которые согласно взгляду SFIA на информационную безопасность, относятся к этой области:

- SCAD: Security administration -> Security operations
- CHMG: Change management -> Change control
- RLMT: Relationship management -> Stakeholder relationship management
- IRMG: Information governance-> Information management

При этом для навыка, поменявшего наименование, код навыка остался тем же.

Девять навыков SFIA были переструктурированы. Элементы уровня ответственности того или иного навыка могли быть перенесены в содержание другого уровня в рамках навыка, или вообще перемещены в описание другого навыка. В частности, среди интересующих нас навыков, прямо или косвенно относящихся к кибербезопасности, был затронут навык Управления данными - Data management (DATM). Некоторые компоненты структуры навыка были перемещены в содержание навыка “Data engineering” (DENG).

IV. Исследование навыков кибербезопасности SIFA

В книге авторов «Модель цифровых навыков кибербезопасности» было проведено исследование актуальной на тот момент версии фреймворка SFIA – SFIA7 [6]. В рамках этого исследования выполнен анализ полноты соответствия связанных с кибербезопасностью международных стандартов куррикулумов компьютинга (признанных на международном уровне учебно-методических материалов системы ИТ-образования) требованиям навыков SFIA7, имеющих отношение к кибербезопасности. Анализ состоял в сравнении на смысловом уровне содержания соответствующих навыков SFIA7 с результатами обучения по указанным куррикулумам. Для проведения такого анализа были выделены две группы навыков стандарта SFIA7, имеющих отношение к подготовке специалистов по кибербезопасности – группы А и Б. В группу А вошли навыки, непосредственно связанные с кибербезопасностью, в группу Б – навыки, поддерживающие решение задач в области информационной безопасности.

В данной статье аналогичный анализ выполнен для новой версии стандарта цифровых навыков SFIA8. Так как в рамках SFIA разработан специальный взгляд SFIA (SFIA view) Информационной и кибербезопасности, объединяющий навыки SFIA8, непосредственно или частично относящиеся к кибербезопасности, проведенный в работе [9] анализ-сравнение с выделением двух групп навыков проведем для навыков из этого взгляда SFIA8.

Цели анализа выделенных групп навыков из взгляда SFIA8 Информационной и кибербезопасности:

1. Составить группы А* и Б* по аналогии с группами навыков А и Б из [9], но на основе множества навыков взгляда Информационной и кибербезопасности SFIA8.
2. Провести анализ групп, аналогичный исследованию [9], с элементами описания навыков.

Сравнение взгляда SFIA Информационная и кибербезопасность с группами А и Б

Во взгляде Информационная и кибербезопасность SFIA8 навыки раздела *Skills for security professionals* непосредственно относятся к области информационной безопасности, что соответствует критерию отбора навыков SFIA7 в группу А. Группу Б будем ассоциировать с навыками SFIA8 остальных разделов взгляда, как имеющие отношение к информационной безопасности частично. Далее сам анализ проведем в два этапа: сравним состав раздела *Skills for security professionals* с составом навыков группы А, а затем проведем аналогичное сравнение для других навыков взгляда и элементов группы Б. В результате исследования получится обновленный состав групп навыков А и Б, которые обозначим как А* и Б* соответственно.

Перечислим состав навыков группы А в сравнении с разделом *Skills for security professionals SFIA8*.

Навыки группы А:

1 Информационная безопасность (Information security) SCTY

2 Информационное обеспечение (Information assurance) INAS

3 Техника безопасности (Safety engineering) SFEN

4 Управление доступностью (Availability management) AVMT

5 Управление безопасностью (Security administration) SCAD

6 Оценка безопасности (Safety assessment) SFAS

7 Цифровая криминалистика (Digital forensics) DGFS

8 Тестирование на проникновение (Penetration testing) PENT

9 Управление информацией (Information governance) IRMG

10 Управление непрерывностью (Continuity management) COPL

Навыки, совпавшие в группе А и первом разделе взгляда SFIA, выделены жирным шрифтом. Подчеркнутый навык, IRMG, вынесен из раздела *Skills for security professionals*, но содержится в другом разделе взгляда SFIA.

Таким образом, выбор навыков группы А согласно исследованию книги [10] отличается от навыков раздела *Skills for security professionals*. Группа А содержит лишь 5 навыков раздела *Skills for security professionals*.

Следующие 4 навыка группы А не попали во взгляд SFIA, в новой версии стандарта они были пересмотрены:

- **SFEN: Техника безопасности (Safety engineering)**
- AVMT: Управление доступностью (Availability management)-
- **SFAS: Оценка безопасности (Safety assessment)+**
- **COPL: Управление непрерывностью (Continuity management) Б**

Среди них навыки с кодами SFAS и SFEN вносятся в группу А*, навык COPL - в группу Б*, AVMT удаляется из групп кибербезопасности.

Один навык из группы А относится к кибербезопасности косвенно по мнению SFIA: это «Управление информацией» (Information governance) IRMG. В нашем случае он включен в группу Б*. В результате 9 из 10 навыков группы А вошли в обойму навыков, определяющих содержание подготовки специалистов по кибербезопасности.

Далее SFIA предлагает 5 новых навыков для использования их в *Skills for security professionals*. Все они появились в содержании фреймворка с выходом SFIA8 и добавлены нами в группу А*:

- AUDT: Аудит (Audit)
- VURE: Изучение уязвимости (Vulnerability research)
- THIN: Анализ угроз (Threat intelligence)
- VUAS: Оценка уязвимости (Vulnerability assessment)
- PEDP: Защита персональных данных (Personal data protection)

Навык RSCH: «Исследование» (Research), предлагаемый SFIA во взгляде, не попадает в новую группу А*.

Перечислим состав группы Б, выделив навыки, попавшие в другие разделы взгляда Информационной и кибербезопасности SFIA8, отличные от *Skills for security professionals*.

Навыки группы Б:

1 Корпоративный ИТ-менеджмент (Enterprise IT governance) GOVN

2 ИТ-менеджмент (IT management) ITMG

3 Архитектура предприятия и бизнеса (Enterprise and business architecture) STPL

4 Управление бизнес-рисками (Business risk management) BURM

5 Архитектура решения (Solution architecture) ARCH

6 Управление данными (Data management) DATM

7 Управление проектами (Project management) PRMG

8 Определение и управление требованиями (Requirements definition and management) REQM

9 Развитие организационных возможностей (Organizational capability development) OCDV

10 Организация: разработка и реализация (Organisation design and implementation) ORDI

11 Управление развитием систем (Systems development management) DLMG

12 Проектирование систем (Systems design) DESN

13 Разработка ПО (Software design) SWDN

14 Программирование/разработка ПО (Programming/software development) PROG

15 Разработка в режиме реального времени / встроенных систем (Real-time/embedded systems development) RESD

16 Разработка баз данных (Database design) DBDS

17 Проектирование сетей (Network design) NTDS

18 Тестирование (Testing) TEST

19 Создание информационного контента (Information content authoring) INCA

20 Дизайн пользовательского интерфейса (User experience design) HCEV

21 Оценка пользовательского опыта (User experience evaluation) USEV

22 Системная интеграция и сборка (Systems integration and build) SINT
23 Проектирование оборудования (Hardware design) HWDE
24 Установка/снятие систем (Systems installation/decommissioning) HSIN
25 Поддержка приложений (Application support) ASUP
26 ИТ-инфраструктура (IT infrastructure) ITOP
27 Администрирование баз данных (Database administration) DBAD
28 Управление хранением (Storage management) STMG
29 Поддержка сети (Network support NTAS)
30 Управление проблемами (Problem management) PBMG
31 Управление инцидентами USUP (Incident management) USUP
32 Управление объектами (Facilities management) DCMA
33 Управление качеством (Quality management) QUMG
~~34 Обзор соответствия (Conformance review) CORE~~
35 Сорсинг (Sourcing) SORC
36 Управление поставщиками (Supplier management) SUPP
37 Консультация специалиста (Specialist advice) TECH
38 Управление знаниями (Knowledge management) KNOW
39 Стратегическое планирование (Strategic planning) ITSP
40 Управление активами (Asset management) ASMG

Анализ группы Б показал большее количество совпадений сравниваемых групп навыков: 25 навыков из 40 попадают во вторичные разделы взгляда SFIA. При этом следует заметить, что пять навыков из группы Б во взгляде SFIA определяются как непосредственно связанные с кибербезопасностью. Эти навыки выделены подчеркиванием. Среди них навыки USUP и AUDT попадают в группу А*, другие в группу Б*.
SFIA предлагает новые навыки для добавления их в группы кибербезопасности:
• SLEN: Проектирование жизненного цикла систем и программного обеспечения (Systems and software life cycle engineering)
• EEXP: Вовлеченность персонала (Employee experience)
• WFPL: Планирование трудовых ресурсов (Workforce planning)

Навык SLEN: «Проектирование жизненного цикла систем и программного обеспечения», определен в группу Б*. Другие 20 навыков, определенные в группе Б, но не попавшие в вышеперечисленные категории, были пересмотрены для включения в группу Б*. В списке они находятся без выделения.
Среди них были исключены из групп кибербезопасности:
1. OCDV: Развитие организационных возможностей (Organisational capability development)
2. ORDI: Организация: разработка и реализация (Organization design and implementation)
3. INCA: Создание информационного контента (Information content authoring)
4. HSIN: Установка/снятие систем (Systems installation/decommissioning)
5. USEV: Оценка пользовательского опыта (User experience evaluation)
6. DBDS: Разработка баз данных (Database design)

Также взгляд SFIA включает в себя ряд неиспользуемых в группах А и Б навыков:

• PGMG: Управление программами (Programme management)
• ETDL: Проведение учебных мероприятий (Learning delivery)
• RELM: Релиз и развертывание (Release and deployment)
• CHMG: Контроль изменений (Change control)
• PEMT: Управление производительностью (Performance management)
• PDSV: Профессиональное развитие (Professional development)
• DEMM: Управление спросом (Demand management)
• RESC: Обеспечение ресурсами (Resourcing)
• LEDA: Оценка компетенций (Competency assessment)
• CNSL: Консалтинг (Consultancy)

Среди них в группу Б* нами включены навыки «Релиз и развертывание» (RELM) и «Контроль изменений» (CHMG).

Таким образом, состав групп А* и Б* представлен ниже.

Навыки группы А*:
1. SCTY: Информационная безопасность (Information security)
2. INAS: Информационное обеспечение (Information assurance)
3. SCAD: Управление безопасностью (Security operations)
4. DGFS: Цифровая криминалистика (Digital forensics)
5. PENT: Тестирование на проникновение (Penetration testing)
6. AUDT: Аудит (Audit)
7. VURE: Изучение уязвимости (Vulnerability research)
8. THIN: Анализ угроз (Threat intelligence)
9. VUAS: Оценка уязвимости (Vulnerability assessment)
10. PEDP: Защита персональных данных (Personal data protection)
11. USUP: Управление инцидентами (Incident management)
12. SFEN: Техника безопасности (Safety engineering)
13. SFAS: Оценка безопасности (Safety assessment)

Навыки группы Б*:
1. GOVN: Системное управление (Governance)
2. STPL: Корпоративная и бизнес-архитектура (Enterprise and business architecture)
3. ITMG: Управление технологическими услугами (Technology service management)

4. BURM: Управление рисками (Risk management)
5. ARCH: Архитектура решений (Solution architecture)
6. DATM: Управление данными (Data management)
7. PRMG: Управление проектами (Project management)
8. REQM: Определение и управление требованиями (Requirements definition and management)
9. DLMG: Управление разработкой систем (Systems development management)
10. DESN: Проектирование систем (Systems design)
11. SWDN: Проектирование ПО (Software design)
12. PROG: Программирование/разработка ПО (Programming/software development)
13. RESD: Разработка систем реального времени / встроенных систем (Real-time/embedded systems development)
14. NTDS: Проектирование сети (Network design)
15. TEST: Тестирование (Testing)
16. HCEV: Проектирование пользовательского опыта (User experience design)
17. SINT: Интеграция и сборка систем (Systems integration and build)
18. HWDE: Проектирование аппаратного обеспечения (Hardware design)
19. ASUP: Поддержка приложения (Application support)
20. ITOP: ИТ инфраструктура (IT infrastructure)
21. DBAD: Администрирование базы данных (Database administration)
22. STMG: Управление хранением (Storage management)
23. NTAS: Поддержка сети (Network support)
24. PBMG: Управление проблемами (Problem management)
25. DCMA: Управление объектами (Facilities management)
26. QUMG: Управление качеством (Quality management)
27. SORC: Сорсинг (Sourcing)
28. SUPP: Управление поставщиками (Supplier management)
29. TECH: Консультация специалиста (Specialist advice)
30. KNOW: Управление знаниями (Knowledge management)
31. ITSP: Стратегическое планирование (Strategic planning)
32. ASMG: Управление активами (Asset management)
33. RELM: Релиз и развертывание (Release and deployment)
34. CHMG: Контроль изменений (Change control)
35. COPL: Управление непрерывностью (Continuity management)
36. IRMG: Управление информацией (Information management)

Анализ навыков SFIA8 групп А и Б**

В работе [10] был проведен анализ современных методических инструментов системы образования, а именно, актуальных куррикулумов, с целью выявления полноты их соответствия требованиям навыков по кибербезопасности. Анализ состоял в сравнении на смысловом уровне содержания навыков SFIA7 с результатами обучения существующих куррикулумов.
В книге для проведения исследования навыки SFIA7 были разбиты на 2 группы: в группу А отнесены навыки, непосредственно связанные с кибербезопасностью, в группу Б – те навыки, в рамках которых решаются отдельные задачи, связанные с информационной безопасностью.

В разделе «*Сравнение взгляда SFIA Информационная и кибербезопасность с группами А и Б*» были собраны новые группы навыков - группы А* и Б*. Навыки этих групп были проанализированы аналогично.
Состав навыков в разрезе знаний и умений, содержание которых не менялось в связи с обовлением фреймворка, перенесен из содержания [10] дословно.
Таким образом, для обновленных в SFIA8 навыков сформулированы требования к знаниям и умениям, представленные в табличном виде.

Пример анализа навыка «Тестирование на проникновение» представлен на рис. 4.

Результаты полного исследования семантики (знаний-умений) навыков кибербезопасности групп А* и Б* размещены в приложении.

Выполненное исследование показало незначительный рост объема требований к знаниям и умениям по сравнению с определенными с помощью модели навыков кибербезопасности (МНК) в работе [10], что, с одной стороны подтверждает практичность разработанной МНК и для новой версии стандарта цифровых навыков SFIA8, а, с другой стороны, может служить основой для актуализации МНК и использующих ее материалов для полного соответствия новой версии стандарта цифровых навыков для информационного века, а именно стандарту SFIA8.

8. Тестирование на проникновение (Penetration testing) PENT	Оценка уязвимостей организации посредством разработки и выполнения тестов на проникновение, которые демонстрируют, как злоумышленник может либо подорвать цели безопасности организации, либо достичь конкретных целей противостояния. Испытание на проникновение может представлять собой отдельное мероприятие или аспект приемочных испытаний до получения разрешения на эксплуатацию. Выявление более глубокого понимания бизнес-рисков различных уязвимостей.	K0 Знание основ куррикулума CSec2017 K1 Знание спектра организационных политик, процессов и защит K2 Объективное понимание наличия уязвимостей, эффективности защитных мер и мер по смягчению последствий - как существующих, так и планируемых к внедрению в будущем K3 Знание об угрозах кибербезопасности K4 Знания требований к среде, данным, ресурсам и инструментам C1 Умение использовать комплексный подход к поиску уязвимостей C2 Умение определить стратегию тестирования C3 Умение управлять процессами тестирования C4 Умение разрабатывать корпоративные стандарты тестирования безопасности C5 Умение создавать тесты, используя углубленный технический анализ рисков и типичных уязвимостей C6 Умение производить тестовые сценарии, материалы и тестовые пакеты для тестирования нового и существующего программного обеспечения или служб C7 Умение интерпретировать, выполнять и документировать сложные тестовые сценарии с использованием согласованных методов и стандартов

Рисунок 4. Анализ навыка «Тестирование на проникновение» [9].

V. Заключение

Процесс глобальной цифровизации способствует появлению большого количесвтва цифровых платформ, направленных на автоматизацию и улучшение многих аспектов нашей жизни. Актуальной задачей является создание цифровой платформы, позволяющей организациям в режиме реального времени публиковать вакансии в терминах стандартизированных навыков, а ВУЗам оперативно реагировать на соответствующие требования работодателей и корректировать текущие программы подготовке специалистов. Такая платформа будет способствовать решению проблемы массового развития востребованных цифровых навыков. Выбор модели описания навыков информационной эры SFIA в качестве методической основы такой платформы гарантирует актуальность содержания цифровых навыков и глобальную применимость.

Результатом выполненного авторами анализа семантики навыков кибербезопасности SFIA8 явилось представление в табличной форме навыков в виде перечней соответствующих им знаний и умений для двух выделенных групп навыков (А* и Б*). Всего были проанализированы 49 навыков, имеющих отношение к решению задач кибербезопасности:

- в группу А* были включены навыки, имеющие прямое отношение к профессии по информационной безопасности (13 навыков),
- в группу Б* - навыки, используемые при решении отдельных задач, связанных с информационной безопасностью (36 навыков).

Сформулированные для навыков из группы А* и группы Б* требования к знаниям и умениям, представлены в приложении. Полученный материал станет основой для обновления куррикулума по кибербезопасности [11], он также будет полезен для методистов и преподавателей при разработке

актуальных учебных программ и курсов, предназначенных для подготовки востребованных специалистов по кибербезопасности.

Библиография

[1] G. O. Young, “Synthetic structure of industrial plastics (Book style with paper title and editor),” in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

[2] Епрев А.С. Автоматическая классификация текстовых документов. Математические структуры и моделирование. 2010. вып. 21, С.65-81.

[3] Полетаева Н.Г. Классификация систем машинного обучения Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. 2020. №1. С. 5-22.

[4] Федюшкин Н. А., Федосин С. А. О выборе методов векторизации текстовой информации. Научно-технический вестник Поволжья. 2019. Т. 6. С. 129-134.

[5] Multi-Lingual Lyrics for Genre Classification https://www.kaggle.com/datasets/mateibejan/multilingual-lyrics-for-genre-classification Дата обращения: 21.02.2022

[6] (10)Dataset Text Document Classification. https://www.kaggle.com/datasets/jensenbaxter/10dataset-text-document-classification. Дата обращения: 21.02.2022

[7] Климов Д.В. Предобработка текстовых сообщений для метрического классифкатора. Символ науки. 2017. №12. С.25-32

[8] Мусаев А. А. и др. Обзор современных технологий извлечения знаний из текстовых сообщений. Компьютерные исследования и моделирование. 2021 Т. 13. № 6. С. 1291–1315 DOI: 10.20537/2076-7633-2021-13-6-1291-1315

[9] Большакова Е.И., Воронцов К.В., Ефремова Н.Э., Клышинский Э.С., Лукашевич Н.В., Сапин А.С. Автоматическая обработка текстов на естественном языке и анализ данных : учеб. пособие. Москва.: Изд-во НИУ ВШЭ. 2017. 269 с.

[10] sklearn.feature_extraction.text.HashingVectorizer, scikit-learn 1.0.2 documentation https://scikit-learn.org/stable/modules/generated/sklearn.feature_extraction.text.HashingVectorizer.html. Дата обращения: 3.04.2022

SFIA8 Cybersecurity Skills Study

O.S. Belyakova, V.A. Sukhomlin

Abstract — **In the context of digitalization of most areas of human activity, the problem of mass training of IT specialists becomes extremely important. In this connection, it seems an urgent task to create a digital platform that allows organizations to report their needs for specialists in real time to fill vacancies in the workplace, and the education system to respond to the relevant needs of employers and offer up-to-date training and retraining programs for in-demand personnel. An example of such a platform is the platform for the development of digital skills, which is being developed as part of the project activities of the laboratory of open information technologies of the faculty of the CMC of Moscow State University. The digital skills standard of the SFIA organization, presented in the form of a framework of the same name, was chosen as the methodological basis of the platform being developed. In September 2021, a new version of the framework was released - SFIA8, which, compared to the previous version of the standard, added two dozen new skills and revised the semantics of a number of skills of the previous version. Also, a characteristic feature of the new stage in the development of the SFIA approach was the development of clusters of roles based on the skills of SFIA (the so-called views of SFIA), corresponding to relevant technological areas, such as, for example, digital transformation, big data, software engineering, cybersecurity, etc. In the first part the article provides an analysis of the main innovations in the SFIA8 standard. The second part is devoted to the study of the semantics (knowledge-abilities) of SFIA8 skills, directly or indirectly related to cybersecurity. In the process of defining the composition of such skills, the skills identified in the SFIA8 Information and Cybersecurity view were primarily considered. The results of the study of the semantics of cybersecurity skills are available in the Appendix. The proposed description of SFIA8 cybersecurity skills in the context of knowledge and abilities is primarily aimed at methodologists and teachers of the education system who develop training programs for professionals in the field of cybersecurity.**

Keywords — **cybersecurity, information security, digital skills, digital skills development platform, SFIA standard.**

REFERENCES

1. Ministerial Declaration: On the Digital Economy: Innovation, Growth and Social Prosperity. [Electronic
resource] - URL: http://www.oecd.org/sti/ieconomy/Digital-Economy-Ministerial-Declaration-2016.pdf
(Date of access: 06/06/2022).
2. Sukhomlin V.A. Who is an IT professional and how to train him / Actual problems of implementing e-
learning and distance learning technologies. Scientific readings. Book I. M: SGU Publishing House, 2015.
125 p. pp.80-99.
3. Sukhomlin, V.A., Namiot D.E., Zubareva E.V., Yakushin A.V., Ilyushin E.A. Multiplatform system for the
development of digital talents "Academy of IT". : Materials of the XII Intern. Scientific and Practical Conf.
"Modern information technologies and IT education" (Moscow, 2017). M: Lomonosov Moscow State
University, 2017.
4. European e-Competence Framework. [electronic resource] - URL: https://www.ecompetences.eu
(date of access: 06.06.2022).
5. IPA: IT Human Resources Development: I Competency Dictionary. / Information Technology
Promotion Agency, Japan. [electronic resource] - URL:
https://www.ipa.go.jp/english/humandev/icd.html (date of access: 06/06/2022)
6. SFIA. [electronic resource] - URL: https://sfia-online.org/en/sfia-8 (date of access: 06/06/2022)
7. Sukhomlin V.A., Zubareva Elena Vasilievna, Namiot D.E., Yakushin A.V. Digital Skills Development
System VMK MSU & Basalt SPO. The methodology for classifying and describing the requirements for
employees and the content of educational programs in the field of information technology. place of
publication Basalt open source software; MAKS Press Moscow, ISBN 978-5-317-06336-8, 184 p.
8. Architecture and principles of curriculum development for the discipline "Cybersecurity" / V.A.
Sukhomlin, O.S. Belyakova, A.S. Klimina, M.S. Polyanskaya. – International scientific journal “Modern
information technologies and IT education”, [S.l.], v. 16, no. 4, 2020. ISSN 2411-1473.
9. Cybersecurity digital skills model 2020 / V.A. Sukhomlin, O.S. Belyakova, A.S. Klimina [i dr.]. –
International scientific journal “Modern information technologies and IT education”, [S.l.], v. 16, no. 3,
nov. 2020. ISSN 2411-1473.
10. Sukhomlin V.A. Model of cybersecurity digital skills: scientific publication / V.A. Sukhomlin, O.S.
Belyakova, A.S. Klimina, M.S. Polyanskaya, A.A. Rusanov. - M: Foundation League of Internet Media,
2021. - 294 p.
11. Sukhomlin V. A. Curriculum of discipline "Cyber security": scientific edition / V. A. Sukhomlin, S. V.
Lebed, O. S. Belyakova, A. S. Klimina, M. S. Polyanskaya. - Moscow: League of Internet Media
Foundation, 2022. - 402 p. – DOI: https://doi.org/10.25559/f6676-8117-2920-j

VI. Приложение: содержание навыков SFIA8, связанных с задачами информационной безопасности

Выделены две группы навыков:

- группу А*, в которую включим навыки, имеющие прямое отношение к профессии по информационной безопасности,

- группу Б*, в которую входят навыки, в рамках которых решаются отдельные задачи, связанные с информационной безопасностью.

В состав группы А* входят следующие навыки:

1. Информационная безопасность (Information security) **SCTY**
2. Информационное обеспечение (Information assurance) **INAS**
3. Управление безопасностью (Security operations) **SCAD**
4. Цифровая криминалистика (Digital forensics) **DGFS**
5. Тестирование на проникновение (Penetration testing) **PENT**
6. Аудит (Audit) **AUDT**
7. Изучение уязвимости (Vulnerability research) **VURE**
8. Анализ угроз (Threat intelligence) **THIN**
9. Оценка уязвимости (Vulnerability assessment) **VUAS**
10. Защита персональных данных (Personal data protection) **PEDP**
11. Управление инцидентами (Incident management) **USUP**
12. Техника безопасности (Safety engineering) **SFEN**
13. Оценка безопасности (Safety assessment) **SFAS**

В состав группы Б* входят следующие навыки:

1. Системное управление (Governance) **GOVN**
2. Корпоративная и бизнес-архитектура (Enterprise and business architecture) **STPL**
3. Управление технологическими услугами (Technology service management) **ITMG**
4. Управление рисками (Risk management) **BURM**
5. Архитектура решений (Solution architecture) **ARCH**
6. Управление данными (Data management) **DATM**
7. Управление проектами (Project management) **PRMG**
8. Определение и управление требованиями (Requirements definition and management) **REQM**
9. Управление разработкой систем (Systems development management) **DLMG**
10. Проектирование систем (Systems design) **DESN**
11. Проектирование ПО (Software design) **SWDN**
12. Программирование/разработка ПО (Programming/software development) **PROG**
13. Разработка систем реального времени / встроенных систем (Real-time/embedded systems development) **RESD**
14. Проектирование сети (Network design) **NTDS**
15. Тестирование (Testing) **TEST**
16. Проектирование пользовательского опыта (User experience design) **HCEV**
17. Интеграция и сборка систем (Systems integration and build) **SINT**
18. Проектирование аппаратного обеспечения (Hardware design) **HWDE**
19. Поддержка приложения (Application support) **ASUP**
20. ИТ инфраструктура (IT infrastructure) **ITOP**
21. Администрирование базы данных (Database administration) **DBAD**
22. Управление хранением (Storage management) **STMG**
23. Поддержка сети (Network support) **NTAS**
24. Управление проблемами (Problem management) **PBMG**
25. Управление объектами (Facilities management) **DCMA**
26. Управление качеством (Quality management) **QUMG**
27. Сорсинг (Sourcing) **SORC**
28. Управление поставщиками (Supplier management) **SUPP**
29. Консультация специалиста (Specialist advice) **TECH**
30. Управление знаниями (Knowledge management) **KNOW**
31. Стратегическое планирование (Strategic planning) **ITSP**
32. Управление активами (Asset management) **ASMG**
33. Релиз и развертывание (Release and deployment) **RELM**
34. Контроль изменений (Change control) **CHMG**

35. Управление непрерывностью (Continuity management) **COPL**
36. Управление информацией (Information management) **IRMG**

В Таблице 1 приводится краткое описание деятельности, выполняемой в рамках навыков группы А, а также соответствующих требований к знаниям и умениям.

Таблица 1

Состав навыков группа А*, описание соответствующего содержания деятельности, а также требований к знаниям и умениям

Навыки	**Активности**	**Знания и умения**
1. Информационная безопасность (Information security) **SCTY**	Выбор, проектирование, обоснование, внедрение и эксплуатация средств контроля и стратегий управления для обеспечения безопасности, конфиденциальности, целостности, доступности, подотчетности и соответствия информационных систем законодательству, нормативным актам и соответствующим стандартам. Осуществляет управление системой информационной безопасности, включая идентификацию ролей и назначение ответственности.	K0 Знание основ куррикулума CSec2017 K1 Знание основных стандартов в области безопасности ИТ, включая: ISO/IEC 27000, ISO/IEC 31000, IEC 61508, ISO/IEC 180281, ISO/IEC 27033-1 K2 Знание стандартов жизненного цикла систем, ПО и услуг: ISO 15288, 12207, 20000 K3 Знание информационной стратегии и политики безопасности организации K4 Понимание возможных угроз безопасности K5 Понимание стратегий мобильности доступа к ресурсам K6 Знание возможностей использования различных моделей обслуживания (SaaS, PaaS, IaaS) C1 Умение разрабатывать и критически анализировать стратегию компании по информационной безопасности C2 Умение определять, представлять и продвигать политику информационной безопасности для утверждения администрацией C3 Умение применять соответствующие стандарты, лучшие практики и юридические требования для информационной безопасности C4 Способность предвидеть необходимые изменения в стратегии информационной безопасности организации и формулировать новые планы C5 Способность предлагать эффективные меры на случай непредвиденных обстоятельств

2. Информационное обеспечение (Information assurance) **INAS**	Защита целостности, доступности, аутентичности, неприкосновенности и конфиденциальности информации и данных в хранилищах и при передаче. Управление рисками прагматичное и экономически эффективное для обеспечения доверия заинтересованных сторон.	K0 Знание основ куррикулума CSec2017 K1 Знание стандартов: ISO 20000, ITIL, ITSM, ISO 55000, 61508 и им аналогичных K2 Знание информационной стратегии и политики безопасности организации K3 Знание международных и национальных стандартов для управления рисками (аналогичных ISO серии ISO 31000) K4 Знание современных методов в области анализа рисков C1 Умение использовать на практике стандарты в области управления активами, оценки функциональной безопасности систем, управления рисками (аналогичных стандартам ISO серий 55000, 61508, 31000) C2 Умение применять современные методы в области анализа рисков на практике C3 Умение применять современные методы защиты целостности, обеспечения доступности, аутентичности, неприкосновенности и конфиденциальности информации и данных в операционных системах, базах данных, компьютерных сетях, облачных технологиях
3. Управление безопасностью (Security operations) **SCAD**	Реализация политики информационной безопасности. Мониторинг и принятие мер против вторжения, мошенничества и нарушений безопасности или утечки информации. Предоставление оперативного управления безопасностью и административными услугами, включая авторизацию и мониторинг доступа к ИТ-средствам или инфраструктуре; расследование несанкционированного доступа и соблюдение соответствующего законодательства; участие в разработке политики безопасности, корпоративных стандартов, процессов и руководств для обеспечения физической и электронной безопасности автоматизированных систем. Несет ответственность за то, что политика	K0 Знание основ куррикулума CSec2017 K1 Знание политики управления безопасностью организации и ее применения при взаимодействии с клиентами, поставщиками и субподрядчиками K2 Знание лучших практик и стандартов в управлении информационной безопасностью K3 Знание методов оценки критических рисков для управления информационной безопасностью K4 Знание процессов проведения внутреннего аудита ИКТ, методов обнаружения нарушения безопасности

	и стандарты для администрирования безопасности соответствуют целям, актуальны и правильно реализованы. Рассматривает новые деловые предложения и предоставляет консультации специалистов по вопросам безопасности и последствиям.	K5 Знание методов проведения кибератак, в том числе с использованием мобильных технологий K6 Знание методов и мер противодействия атакам K7 Знание методов компьютерной криминалистики C1 Умение документировать политику управления информационной безопасностью, связывая ее с бизнес-стратегией C2 Владение методами защиты критически важных активов компании и выявления их уязвимостей для вторжения или атаки C3 Умение разработать план управления рисками для обеспечения и разработки планов превентивных действий C4 Умение выполнить аудит безопасности C5 Владение методами мониторинга и тестирования процессов на соответствие политики безопасности C6 Умение планировать восстановление после аварий C7 Способность осуществлять план восстановления в случае кризиса
4. Цифровая криминалистика (Digital forensics) **DGFS**	Сбор, обработка, сохранение, анализ и представление судебных доказательств на основе совокупности результатов, включая компьютерные доказательства, в поддержку мер по снижению уязвимости безопасности и / или расследований по уголовным делам, мошенничеству, контрразведке или правоохранительным органам. Устанавливает политики, стандарты и руководящие принципы для того, как организация проводит цифровые судебные расследования. Руководит и управляет сложными расследованиями, привлекая дополнительных специалистов при необходимости. Разрешает выпуск официальных отчетов судебно-медицинской экспертизы. Проводит расследования для правильного сбора, анализа и представления всей совокупности результатов, включая цифровые	K0 Знание основ куррикулума CSec2017 K1 Знание основ криминалистики, включая: - принцип Locard, способы физической передачи признаков, методы ассоциации и реконструкции событий - методы цифровых доказательств нарушения целостности и подлинности, определения носителей доказательств - методы регистрации и сохранения цифровых доказательств K3 Типы данных: первичные, вторичные, программные, конфигурационные, журналы / протоколы C1 Умение применять методы

	доказательства, как деловой, так и юридической аудитории. Собирает выводы и рекомендации и представляет результаты судебной экспертизы заинтересованным сторонам. Способствует разработке политики, стандартов и руководств.	анализа и средства обнаружения повреждения данных, нарушения целостности / подлинности C2 Умение извлекать свидетельства, анализировать файлы журналов C3 Владение методами цифровой криминалистики, включая: TriageIR, TR3Secure, Kludge, методы сортировки диска C4 Выполнение этапов криминалистической экспертизы: (a) что произошло, (б) где, (в) когда, (г) как; потенциально (e) атрибуция (кем), (f) как предотвратить в будущем C5 Умение выполнять экспертизу файлов, кодировку, анализ заголовков файлов и метаданных C6 Умение выполнять экспертизу электронной почты (анализ заголовков, методы SPF, DMARC, DKIM) C7 Умение выполнять RAM-экспертизу (волатильность) C8 Умение выполнять сетевую экспертизу, анализ потока C9 Владение методами и инструментами (Imaging Live Imaging, например, ftk imager) C10 Владение методами тестирования на шифрование, например ЭДД C11 Владение вспомогательными инструментами: IDS (хост / сеть), неизменяемые логи C12 Владение методами анализа вредоносных программ C13 Владение методами статического анализа C14 Владение методами динамического анализа C15 Владение методами Malware Sandbox / автоматический анализ C16 Владение методами анти-анализа
5. Тестирование на	Оценка уязвимостей организации	K0 Знание основ куррикулума

проникновение (Penetration testing) **PENT**	посредством разработки и выполнения тестов на проникновение, которые демонстрируют, как злоумышленник может либо подорвать цели безопасности организации, либо достичь конкретных целей противостояния. Испытание на проникновение может представлять собой отдельное мероприятие или аспект приемочных испытаний до получения разрешения на эксплуатацию. Выявление более глубокого понимания бизнес-рисков различных уязвимостей.	CSec2017 K1 Знание спектра организационных политик, процессов и защит K2 Объективное понимание наличия уязвимостей, эффективности защитных мер и мер по смягчению последствий - как существующих, так и планируемых к внедрению в будущем K3 Знание об угрозах кибербезопасности K4 Знания требований к среде, данным, ресурсам и инструментам C1 Умение использовать комплексный подход к поиску уязвимостей C2 Умение определить стратегию тестирования C3 Умение управлять процессами тестирования C4 Умение разрабатывать корпоративные стандарты тестирования безопасности C5 Умение создавать тесты, используя углубленный технический анализ рисков и типичных уязвимостей C6 Умение производить тестовые сценарии, материалы и тестовые пакеты для тестирования нового и существующего программного обеспечения или служб C7 Умение интерпретировать, выполнять и документировать сложные тестовые сценарии с использованием согласованных методов и стандартов
6. Аудит (Audit) **AUDT**	Независимая оценка соответствия любой деятельности, процесса, результата, продукта или услуги критериям указанных стандартов, наилучшей практики или других задокументированных требований. Может относиться, например, к управлению активами, инструментам сетевой безопасности, брандмауэрам и интернет-безопасности, устойчивости, системам реального времени, разработке приложений и специальным сертификатам.	K0 Знание стандартов, нормативных актов и законодательства соответствующей сферы C1 Умение оценивать соответствие конкретной деятельности или результата (например, инструментов сетевой безопасности) критериям указанных стандартов C2 Умение определить организационные процедуры для сторонней оценки деятельности или результата C3 Умение определить зоны риска и способствовать их уменьшению C4 Умение собирать, сопоставлять, проверять и анализировать записи в рамках определенных стратегий

		тестирования на предмет подтверждения соответствия директивам управления или выявления аномальных явлений
7. Изучение уязвимости (Vulnerability research) **VURE**	Проведение прикладных исследований для обнаружения, оценки и смягчения новых или неизвестных уязвимостей и слабых мест в системе безопасности. Деятельность может включать, но не ограничиваться: ▪ изучение новых угроз, векторов атак, рисков и потенциальных решений ▪ обратное проектирование оборудования или программного обеспечения ▪ применение таких инструментов, как дизассемблеры, отладчики и фаззеры ▪ анализ встроенных устройств ▪ разработка методов и инструментов для анализа и выявления уязвимостей ▪ разработка новых методов обнаружения уязвимостей ▪ обмен методами смягчения последствий с соответствующими заинтересованными сторонами.	K1 Знание существующих угроз и уязвимостей K2 Знание методов исследования и оценки уязвимостей C1 Умение разработать и выполнить сложные стратегии исследования уязвимостей C2 Умение применять стандартные методы и инструменты исследования уязвимостей C3 Умение оценивать и документировать угрозы организации
8. Анализ угроз (Threat intelligence) **THIN**	Разработка и распространение практической информации о текущих и потенциальных угрозах безопасности для успеха или целостности организации. Деятельность может включать, но не ограничиваться: ▪ сбор данных из различных открытых или проприетарных источников разведки ▪ обработка и классификация данных об угрозах для того, чтобы сделать их полезными и пригодными для действий других лиц ▪ упаковка данных для использования потребителями информации ▪ обеспечение возможности автоматического использования данных средствами безопасности	K1 Знание методов исследования уязвимостей C1 Умение применять стандартные инструменты исследования уязвимостей C2 Умение разработать и выполнить сложные стратегии исследования уязвимостей C3 Умение проводить тестирование среды на наличие уязвимостей

	▪ предоставление информации об угрозах, чтобы помочь другим уменьшить уязвимость или отреагировать на инциденты безопасности.	
9. Оценка уязвимости (Vulnerability assessment) **VUAS**	Выявление и классификация уязвимостей безопасности в сетях, системах и приложениях и смягчение или устранение их влияния. Деятельность может включать, но не ограничиваться: ▪ каталогизация и классификация информационных и технологических ресурсов (активов и возможностей) для поддержки оценки уязвимости ▪ присвоение количественной ценности, порядка ранжирования и важности информационным и технологическим ресурсам ▪ выявление и анализ уязвимостей каждого ресурса - вручную или с использованием автоматизированных инструментов и источников информации ▪ определение приоритетов, подсчет баллов и ранжирование рисков, связанных с уязвимостями ▪ оценка влияния на бизнес ▪ смягчение или устранение уязвимостей. Инструменты оценки уязвимостей включают сканеры веб-приложений, сканеры протоколов и сетевые сканеры.	K1 Знание стандартных методов анализа и оценки уязвимостей K2 Знание различных инструментов оценки уязвимости C1 Умение провести базовую оценку уязвимостей информационной системы C2 Умение применять инструменты оценки уязвимостей
10. Защита персональных данных (Personal data protection) **PEDP**	Внедрение и функционирование системы контроля и стратегий управления для обеспечения соответствия законодательству о персональных данных. Деятельность может включать, но не ограничиваться: ▪ предоставление экспертных консультаций по вопросам политики, процедур и управления ▪ разработка продуктов, услуг	K1 Знание стандартов и руководств, связанных с законодательством о персональных данных C1 Умение расследовать нарушения данных C2 Умение вести реестр данных, попадающих под действие законодательства о персональных данных C3 Умение провести оценку рисков

	и систем, обеспечивающих конфиденциальность, которые уважают частную жизнь клиентов и обеспечивают защиту данных ▪ проведение оценки воздействия, выявление рисков, обеспечивая при этом разумное использование данных и решение проблем с продуктами и услугами ▪ реагирование на инциденты ▪ следующие изменения в законодательстве ▪ создание моделей и фреймворков риска для конфиденциальности ▪ работа с экспертами в таких областях, как - но не ограничиваясь ими - юридическая, связи с общественностью, обучение и развитие, закупки, безопасность, управление данными, архитектура.	С4 Умение разработать стратегии по соблюдению законодательства о персональных данных, отследить их актуальность и правильность применения
11. Управление инцидентами (Incident management) **USUP**	Обработка и координация соответствующих и своевременных ответов на отчеты об инцидентах, включая направление запросов о помощи в соответствующие функции для разрешения, мониторинг действий по разрешению и информирование клиентов о прогрессе в восстановлении услуг.	К1 Знание методов эффективного восстановления после разрешения инцидентов С1 Умение установить приоритеты и диагностировать инциденты в соответствии с согласованными процедурами, найти причины инцидентов и способствовать их разрешению С2 Умение анализировать причины инцидентов, показатели и отчеты о результатах процесса управления инцидентами
12. Техника безопасности (Safety engineering) **SFEN**	Применение соответствующих методов для обеспечения безопасности на всех этапах жизненного цикла разработки систем, связанных с безопасностью. Деятельность может включать, но не ограничиваться: ▪ анализ опасностей и рисков для безопасности ▪ спецификация требований безопасности ▪ архитектурное проектирование систем, связанных с безопасностью	К1 Знание стандартов безопасности IEC 61508, IEC 61511, технических стандартов и стандартов качества С1 Умение провести анализ угроз и рисков при разработке и внедрении системы С2 Умение документировать результаты анализа угроз и рисков С3 Умение обосновать безопасность, собрать доказательства обеспечение безопасности

	▪ разработка формальных методов ▪ валидация и верификация безопасности ▪ подготовка обоснования безопасности ▪ применение общих стандартов безопасности, таких как IEC 61508, IEC 61511 или отраслевых стандартов безопасности. Безопасность системы проектируется и измеряется уровнями безопасности, основанными на анализе опасностей и рисков.	
13. Оценка безопасности (Safety assessment) **SFAS**	Оценка программных и аппаратных систем, связанных с безопасностью, для определения соответствия стандартам и требуемым уровням целостности безопасности. Деятельность может включать, но не ограничиваться: ▪ вынесение профессиональных суждений о подходах к проектированию программного и аппаратного обеспечения ▪ оценка пригодности методов проектирования, тестирования, а также валидации и верификации ▪ выявление и оценка рисков и способов их снижения ▪ создание, поддержание и управление системой и практикой оценки безопасности ▪ с использованием таких методов, как анализ влияния режимов отказов, исследования опасности и работоспособности, анализ влияния отказов компонентов, анализ дерева отказов, анализ дерева событий и анализ критичности.	К1 Знание методов доказательства обеспечения безопасности К2 Знание стандартов безопасности, технических стандартов, стандартов качества С1 Умение применить инструменты сбора доказательств обеспечения безопасности С2 Умение провести анализ безопасности для проверки или подтверждения вполнения требований безопасности С3 Умение создать отчет по оценке безопасности

В Таблице 2 приводится краткое описание деятельности, соответствующей навыкам группы Б*, а также соответствующих требований к знаниям и умениям, необходимым для решения задач, связанных с обеспечением информационной безопасности.

Таблица 2

Состав навыков группы Б*, описание соответствующего содержания деятельности, а также требований к знаниям и умениям для решения задач, связанных с обеспечением информационной безопасности

Навыки	**Активности**	**Знания и компетенции в области ИБ**
1. Системное управление (Governance) **GOVN**	Создание и надзор за подходом организации к использованию информационных систем и цифровых услуг и связанных с ними технологий в соответствии с потребностями основных заинтересованных сторон организации и общими требованиями корпоративного управления организации. Определение и ответственность за оценку текущих и будущих потребностей; руководство планированием как предложение, так и спроса на эти услуги; качество, характеристики и уровень ИТ-услуг; и для мониторинга соответствия обязательствам (включая нормативные, законодательные, контрольные и другие стандарты) для обеспечения положительного вклада ИТ в цели и задачи организации. Руководство созданием и обслуживанием функции, обеспечивающей согласованный и интегрированный подход к управлению ИТ в соответствии с требованиями корпоративного управления организации. На самом высоком уровне в деятельности по управлению организацией обеспечивает основные заинтересованные стороны гарантией того, что ИТ-службы выполняют обязательства организации (включая законодательство, нормативные, договорные и согласованные стандарты / политики). Отвечает за то, что рамки политики, стандартов, процессов и практик обеспечивают руководство предоставлением необходимых корпоративных ИТ-услуг, и что реализуется надлежащий мониторинг структуры управления. Осуществляет руководство, обеспечивающее прозрачность принятия решений, работая с руководителями высшего звена, чтобы обеспечить понимание потребностей основных	К1 Знание стандартов/правил, необходимых для соблюдения обязательств организации К2 Знание системы политик, стандартов, процессов и практик, необходимых для руководства предоставлением корпоративных ИТ-услуг С1 Умение устанавливать и поддерживать политику соблюдения обязательств организации. С2 Умение обеспечивать наличие надлежащих отношений между организацией и внешними сторонами, проявляющими интерес к управлению организацией. С3 Умение работать со старшими руководителями, чтобы обеспечивать понимание потребностей основных заинтересованных сторон

	заинтересованных сторон, ценностное предложение, предлагаемое корпоративными ИТ.	
2. Корпоративная и бизнес-архитектура (Enterprise and business architecture) **STPL**	Создание, итерация и обслуживание структур, таких как корпоративные и бизнес-архитектуры, воплощающие ключевые принципы, методы и модели, которые описывают будущее состояние организации и обеспечивают ее развитие. Это обычно включает в себя интерпретацию бизнес-целей и драйверов; перевод бизнес-стратегии и целей в «операционную модель»; стратегическая оценка текущих возможностей; выявление необходимых изменений в возможностях; и описание взаимоотношений между людьми, организацией, службой, процессом, данными, информацией, технологиями и внешней средой. Процесс разработки архитектуры поддерживает формирование ограничений, стандартов и руководящих принципов, необходимых для определения, обеспечения и управления требуемой эволюцией; это облегчает изменение структуры организации, бизнес-процессов, систем и инфраструктуры для достижения предсказуемого перехода к предполагаемому состоянию.	K1 Знание рыночных и экологических тенденций, бизнес-стратегий и целей, а также преимуществ альтернативных стратегий C1 Умение создавать стратегии системного потенциала, отвечающие стратегическим требованиям бизнеса C2 Умение разрабатывать модели и планы управления реализацией стратегии, используя возможности повышения эффективности бизнеса C3 Умение разрабатывать бизнес-кейсы для инициатив высокого уровня, утверждения, финансирования и определения приоритетов C4 Умение контролировать соответствие между бизнес-стратегиями, действиями по трансформации предприятий и технологическими направлениями, установлением стратегий, политик, стандартов и практик
3. Управление технологическими услугами (Technology service management) **ITMG**	Управление ИТ-инфраструктурой и ресурсами, необходимыми для планирования, разработки, предоставления и поддержки ИТ-услуг и продуктов для удовлетворения потребностей бизнеса. Подготовка к новым или измененным услугам, управление процессом изменений и поддержание нормативных, правовых и профессиональных стандартов. Управление производительностью систем и услуг с точки зрения их вклада в эффективность бизнеса, их финансовых затрат и устойчивости. Управление покупными услугами. Разработка планов непрерывного совершенствования услуг для	K0 Знание стратегий мониторинга и управления производительностью технологических ресурсов, связанных с информационной безопасностью C1 Умение распределять ресурсы для планирования, разработки, предоставления и поддержки всех информационных систем и продуктов C2 Умение управлять проектированием, закупкой, установкой, модернизацией, эксплуатацией, контролем, техническим обслуживанием (включая хранение, модификацию и передачу данных, голоса, текста, аудио и изображений) C3 Умение эффективно использовать компоненты

	обеспечения адекватной поддержки ИТ-инфраструктуры потребностями бизнеса.	ИТ-инфраструктуры и контролировать их работу
4. Управление рисками (Risk management) **BURM**	Планирование и внедрение общеорганизационных процессов и процедур для управления риском для успеха или целостности бизнеса, особенно тех, которые связаны с использованием информационных технологий, сокращением или отсутствием энергоснабжения или ненадлежащей утилизацией материалов, оборудования или данные.	K0 Знание потенциальных рисковых событий в рамках информационной безопасности K1 Знание контрмер и планов действий в чрезвычайных ситуациях K3 Знание методов выявления, оценки и управления рисками K4 Знание стратегий устранения рисков C0 Умение выявить потенциальные рисковые события C1 Умение давать оценку вероятности возникновения рисковых ситуаций C2 Умение документировать и оценивать влияние на бизнес возникновения рисковых ситуаций C3 Умение планировать и управлять внедрением общеорганизационных процессов и процедур, инструментов и методов для выявления, оценки и управления рисками
5. Архитектура решений (Solution architecture) **ARCH**	Проектирование и коммуникация структур высокого уровня для обеспечения и руководства проектированием и разработкой интегрированных решений, отвечающих текущим и будущим потребностям бизнеса. В дополнение к технологическим компонентам архитектура решения включает в себя изменения в сервисах, процессах, организации и операционных моделях. Предоставление исчерпывающего руководства по разработке и модификации компонентов решения для обеспечения того, чтобы они учитывали соответствующие архитектуры, стратегии, политики, стандарты и практики (включая безопасность) и чтобы существующие и планируемые компоненты решения оставались совместимыми.	K0 Знание технических стратегий, политик, стандартов (корпоративных, отраслевых, национальных и международных) и практик (включая безопасность) C1 Умение поддерживать изменения проекта путём подготовки технических планов и применения принципов проектирования
6. Управление данными (Data management) **DATM**	Управление практиками и процессами для обеспечения безопасности, качества, целостности, безопасности и доступности всех форм данных и структур данных, составляющих	K1 Знание способов преобразования данных/информации из одного формата или носителя в другой K2 Знание способов эффективного хранения, обмена

	информацию организации. Управление данными и информацией во всех ее формах и анализ информационной структуры (включая логический анализ таксономий, данных и метаданных). Разработка инновационных способов управления информационными активами организации.	и публикации данных внутри организации С1 Умение оценить целостность данных из нескольких источников С2 Умение использовать конкретные данные из информационных служб, чтобы удовлетворить определенные информационные потребности С3 Умение создавать структуры управления данными и метаданные для обеспечения согласованности поиска, комбинирования, анализа, распознавания образов и интерпретации информации во всей организации С4 Умение разработать организационную политику, стандарты и руководящие принципы управления данными, соответствующие этическим принципам
7. Управление проектами (Project management) **PRMG**	Управление проектами, обычно (но не исключительно), включающими разработку и внедрение бизнес-процессов для удовлетворения выявленных бизнес-потребностей, приобретение и использование необходимых ресурсов и навыков в рамках согласованных параметров стоимости, сроков и качества. Принятие и адаптация методологий управления проектами на основе контекста проекта и соответствующего выбора из прогнозирующих (управляемых планом) подходов или адаптивных (итеративных / гибких) подходов.	К0 Знание эффективных процессов контроля проекта, контроля изменений, управления рисками и тестирования С1 Умение управлять рисками и обеспечивать решение проблем в соответствии с процессами контроля изменений С2 Умение реализовать эффективные процессы контроля проекта, контроля изменений, управления рисками и тестирования
8. Определение и управление требованиями (Requirements definition and management) **REQM**	Выявление, анализ, спецификация и проверка требований и ограничений до уровня, позволяющего эффективно разрабатывать и эксплуатировать новое или измененное программное обеспечение, системы, процессы, продукты и услуги. Управление требованиями на протяжении всего жизненного цикла поставки и эксплуатации программного обеспечения, системы, процессов, продуктов или услуг. Переговоры о компромиссах, приемлемых как для ключевых заинтересованных сторон, так и в рамках бюджетных, технических, нормативных и других	К1 Знание прогнозных (управляемых планом) подходов и адаптивных (итеративных/гибких) подходов С1 Умение определить и масштабы, требования и приоритеты для инициатив среднего размера и сложности С2 Умение выбирать, принимать и адаптировать определения требований и управления, инструменты и методы, соответствующим образом выбираемые из прогнозных (управляемых планом) подходов или адаптивных (итеративных/гибких) подходов С3 Умение разработать организационную политику, стандарты и руководящие

	ограничений. Принятие и адаптация моделей жизненного цикла управления требованиями на основе контекста работы и соответствующего выбора из плановых / прогнозных подходов или более адаптивных (итеративных и гибких) подходов.	принципы для определения требований и управления ими
9. Управление разработкой систем (Systems development management) **DLMG**	Планирование, оценка и выполнение программ разработки систем с учетом временных, бюджетных и качественных показателей. Определение ресурсов, необходимых для разработки систем, и того, как это будет достигнуто при эффективном объеме поставок. Согласование деятельности по разработке систем и результатов с согласованными архитектурами и стандартами. Разработка дорожных карт для сообщения о будущих планах развития систем. Принятие и адаптация моделей жизненного цикла разработки систем на основе контекста работы и соответствующего выбора из прогнозирующих (управляемых планом) подходов или адаптивных (итеративных / гибких) подходов.	K0 Знание методов разработки систем, инструментов, в том числе в рамках безопасности C1 Умение обосновать преимущества решения всех проблем безопасности во время разработки систем, продвижение таких решений C2 Умение обеспечить выполнение проектов в соответствии с согласованными архитектурами, стандартами, методами и процедурами (включая безопасную разработку программного обеспечения)
10. Проектирование систем (Systems design) **DESN**	Проектирование систем в соответствии с указанными требованиями, совместимость с согласованными системными архитектурами, соблюдение корпоративных стандартов и в рамках ограничений производительности и выполнимости. Выявление концепций и их перевод в проект, который служит основой для построения и проверки систем. Дизайн или подбор комплектующих. Разработка полного набора подробных моделей, свойств и / или характеристик описана в форме, подходящей для реализации. Принятие и адаптация моделей жизненного цикла проектирования систем на основе контекста работы и соответствующего выбора из прогнозирующих (проверенных) подходов или адаптивных (итеративных / гибких) подходов. Разрабатывает	K1 Знание прогнозных (управляемых планом) подходов или адаптивных (итеративных/гибких) подходов K2 Знание стандартов, руководящих принципов и методов проектирования систем C1 Умение проектировать компоненты с использованием соответствующих методов моделирования в соответствии с согласованными архитектурами, стандартами проектирования, шаблонами и методологией C2 Умение моделировать поведение предлагаемых компонентов систем C3 Умение разработать эффективную организационную политику, стандарты, руководящие принципы и методы проектирования систем C4 Умение разработать проекты систем, требующих внедрения новых технологий или нового использования существующих технологий

	организационную политику, стандарты, руководства и методы проектирования систем. Отстаивает важность и ценность принципов проектирования систем и выбора соответствующих моделей жизненного цикла проектирования систем; будь то прогнозирующие (управляемые планом) подходы или более адаптивные (итеративные / гибкие) подходы. Приводит к принятию и соблюдению соответствующих политик, стандартов, стратегий и архитектур. Руководит проектированием систем для стратегических, крупных и сложных программ разработки систем. Разрабатывает эффективные стратегии внедрения и закупок, соответствующие указанным требованиям, архитектурам и ограничениям производительности и осуществимости. Разрабатывает конструкции систем, требующие внедрения новых технологий или новых применений существующих технологий.	
11. Проектирование ПО (Software design) **SWDN**	Проектирование систем в соответствии с указанными требованиями, совместимость с согласованными системными архитектурами, соблюдение корпоративных стандартов и в рамках ограничений производительности и выполнимости. Выявление концепций и их перевод в проект, который служит основой для построения и проверки систем. Дизайн или подбор комплектующих. Разработка полного набора подробных моделей, свойств и / или характеристик описана в форме, подходящей для реализации. Принятие и адаптация моделей жизненного цикла проектирования систем на основе контекста работы и соответствующего выбора из прогнозирующих (проверенных) или адаптивных (итеративных / гибких) подходов	K0 Знание требований к функциональности, качеству, безопасности и управлению системами при проектировании системы K1 Знание организационных политик и стандартов проектирования и архитектуры программного обеспечения K2 Знание сторонних разработок C1 Умение обеспечивать соблюдение технических стратегий и архитектур систем (включая безопасность) C2 Умение проводить анализ воздействия на основные варианты проектирования, давать рекомендации, оценивать связанные с ними риски и управлять ими C3 Умение оценить качество проектирования других систем для обеспечения соблюдения стандартов C4 Умение разрабатывать программные компоненты и модули с использованием соответствующих методов моделирования в соответствии с согласованными стандартами

		проектирования программного обеспечения, шаблонами и методологией С5 Умение рекомендовать проекты, учитывающие целевую среду, требования безопасности производительности и существующие системы
12. Программирование/разработка ПО (Programming/software development) **PROG**	Планирование, проектирование, создание, внесение изменений, проверка, тестирование и документирование новых и измененных программных компонентов для обеспечения согласованной ценности для заинтересованных сторон. Выявление, создание и применение согласованных стандартов и процессов разработки программного обеспечения и безопасности. Принятие и адаптация моделей жизненного цикла разработки программного обеспечения на основе контекста работы и соответствующий выбор из прогнозирующих (управляемых планом) подходов или адаптивных (итеративных / гибких) подходов.	К1 Знание прогнозных (управляемых планом) подходов или адаптивных (итеративных/гибких) подходов К2 Знание стандартов и процессов разработки программного обеспечения и обеспечения безопасности С1 Умение проектировать, кодировать, проверять, тестировать, документировать, вносить изменения и редактировать сложные программы / скрипты и интеграционные программные сервисы С2 Умение контролировать применение стандартов проекта / команды для построения программного обеспечения, включая безопасность программного обеспечения С3 Умение руководить разработкой программного обеспечения для стратегических, крупных и сложных исследовательских проектов
13. Разработка систем реального времени / встроенных систем (Real-time/embedded systems development) **RESD**	Архитектура, проектирование и разработка надежного программного обеспечения, операционных систем, инструментов и встроенных систем реального времени. Встраивание компьютерных систем с выделенной функцией в более крупную механическую или электронную систему, часто с ограничениями реального времени, безопасности, надежности и надежности. Обычно включает взаимодействие с оборудованием, механическими датчиками и исполнительными механизмами для мониторинга и управления в таких приложениях, как промышленное, автомобильное, аэрокосмическое и медицинское оборудование, роботы и оборудование, включая устройства IoT (Internet of Things).	К0 Знание методов валидации и проверки К1 Знание требований к производительности, безопасности, надежности систем реального времени и встроенных систем С1 Умение внести вклад в деятельность по валидации и проверке С2 Умение провести анализ влияния основных вариантов проектирования и компромиссов между аппаратным и программным обеспечением С3 Умение оценить проекты других компаний, чтобы обеспечить выбор соответствующих компонент и эффективное использование ресурсов
14. Проектирование сети	Производство сетевых проектов	К1 Знание процедур проверки и

(Network design) **NTDS**	и политик проектирования, стратегий, архитектур и документации, охватывающих передачу голоса, данных, текста, электронной почты, факсимильной связи и изображений, для поддержки требований стратегии и бизнеса в отношении подключения, пропускной способности, взаимодействия, безопасности, устойчивости, восстановления, доступа и удаленный доступ. Это может включать в себя все аспекты инфраструктуры связи, внутренние и внешние, мобильные, публичные и частные, Интернет, Интранет и центры обработки вызовов.	исправления ошибок, правил обработки, средств контроля доступа, безопасности и аудита К2 Знание сетевых архитектур, топологий и конфигурации поставщиков сетевых услуг С1 Создание эскизных проектов систем и спецификаций, а также общих архитектур и проектной документации сетей и сетевых технологий С2 Умение создавать интерфейсы пользователя, включая средства контроля доступа и безопасности С3 Умение оценивать связанные с интерфейсом пользователя риски и определять процедуры восстановления на случай непредвиденных обстоятельств
15. Тестирование (Testing) **TEST**	Планирование, проектирование, управление, выполнение и отчетность испытаний, с использованием соответствующих инструментов и методов тестирования и в соответствии с согласованными стандартами процесса и отраслевыми правилами. Цель тестирования - убедиться, что новые и исправленные системы, конфигурации, пакеты или сервисы вместе с любыми интерфейсами работают так, как указано (включая требования безопасности), и что риски, связанные с развертыванием, адекватно поняты и задокументированы.	К1 Знание соответствующих инструментов и методов испытаний и в соответствии с согласованными технологическими стандартами и отраслевыми нормативами К2 Знание процесса разработки, использования и поддержания тестового программного обеспечения (тестовые кейсы, тестовые сценарии, отчеты о тестировании, планы тестирования и т. д.) К3 Знание уровня практичности альтернативных процессов тестирования, включая автоматизированное тестирование С1 Умение производить тестовые сценарии, материалы и пакеты регрессионных тестов для тестирования нового и измененного программного обеспечения или служб С2 Умение интерпретировать, выполнять и документировать сложные тестовые сценарии с использованием согласованных методов и стандартов С3 Умение координировать планирование системы и / или приемочные испытания, включая тестирование безопасности программного обеспечения, в рамках проекта или программы разработки или интеграции
16. Проектирование пользовательского опыта (User experience design) **HCEV**	Процесс итеративного проектирования для повышения удовлетворенности пользователей за счет повышения удобства использования и доступности, предоставляемых при	К1 Знание необходимых инструментов, методов и шаблонов проектирования С1 Умение проектировать цифровые и автономные задачи пользователей, взаимодействие и интерфейсы для удовлетворения

	взаимодействии с системой, продуктом или услугой. Разработка цифровых и автономных задач, взаимодействий и интерфейсов пользователей для удовлетворения требований удобства использования и доступности. Уточнение дизайна в ответ на оценку, ориентированную на пользователя, а также обратную связь и передачу проекта лицам, ответственным за проектирование, разработку и реализацию.	согласованных требований к удобству использования и доступности C2 Умение оценить альтернативные варианты проектирования с учетом требований к производительности, удобству использования и доступности C3 Умение использовать итерационные подходы для быстрого включения обратной связи с пользователями в проекты
17. Интеграция и сборка систем (Systems integration and build) **SINT**	Планирование, реализация и контроль действий по интеграции / созданию компонентов, подсистем и интерфейсов для создания операционных систем, продуктов или услуг для доставки клиентам или для внутренних или промежуточных целей, таких как тестирование. Развитие организационных возможностей для системной интеграции и сборки, включая автоматизацию и непрерывную интеграцию.	K1 Знание инструментов, методов и процессов (включая автоматизацию и непрерывную интеграцию) создания надежной структуры интеграции C1 Умение проектировать и выполнять испытания интеграционной сборки C2 Умение создавать интеграционные компоненты и интерфейсы C3 Умение контролировать деятельность по интеграции/созданию компонентов, подсистем и интерфейсов для создания операционных систем, продуктов или услуг для доставки клиентам
18. Проектирование аппаратного обеспечения (Hardware design) **HWDE**	Спецификация и проектирование вычислительного и коммуникационного оборудования (такого как полупроводниковые процессоры, архитектуры HPC и микросхемы DSP и графических процессоров), обычно для интеграции в ИТ-инфраструктуру или сеть или подключения к ней. Выявление концепций и их перевод в реализуемый дизайн. Выбор и интеграция, или дизайн и создание прототипов компонентов. Соблюдение отраслевых стандартов, включая совместимость, безопасность и устойчивость.	K0 Знание технических стратегий, политик, стандартов и практик K1 Знание стандартов проектирования, методов и инструментов, соответствующих согласованной политике предприятия C1 Умение обеспечить эффективное применение стандартов проектирования, методов и инструментов, соответствующих согласованной политике предприятия C1 Умение оценивать и управлять связанными с ними рисками, связанными с основными вариантами проектирования C3 Умение проектировать вычислительное и коммуникационное оборудование с учетом требований целевой среды, производительности, безопасности и устойчивости C4 Умение проектировать тесты

		для измерения производительности прототипов и выхода продукции в соответствии со спецификацией
19. Поддержка приложения (Application support) **ASUP**	Предоставление услуг по обслуживанию и поддержке приложений либо непосредственно пользователям систем, либо функциям доставки услуг. Поддержка обычно включает в себя расследование и решение проблем, а также может включать мониторинг производительности. Проблемы могут быть решены путем предоставления рекомендаций или обучения пользователям, путем разработки исправлений (постоянных или временных) для сбоев, внесения общих или специфических для сайта изменений, обновления документации, манипулирования данными или определения улучшений. Поддержка часто предполагает тесное сотрудничество с разработчиками системы и / или с коллегами, специализирующимися в различных областях, таких как база данных, администрация или поддержка сети.	K1 Знание вопросов безопасности приложений, лицензирования, обновления, резервного копирования и аварийного восстановления C1 Умение использовать программное обеспечение и инструменты управления приложениями для изучения проблем, сбора статистики производительности и создания отчетов C2 Умение разрабатывать процедуры и документацию для поддержки приложений.
20. ИТ инфраструктура (IT infrastructure) **ITOP**	Функционирование и управление ИТ-инфраструктурой (включая физическое или виртуальное оборудование, программное обеспечение, сетевые службы и хранилище данных) либо локально, либо в виде облачных служб), которая требуется для предоставления и поддержки потребностей информационных систем бизнеса. Включает подготовку к новым или измененным услугам, управление процессом изменений, поддержание нормативных, правовых и профессиональных стандартов, создание и управление системами и компонентами в виртуализированных и облачных вычислительных средах, а также мониторинг производительности систем и услуг в отношении их вклада в эффективность бизнеса, их безопасность и устойчивость. Применение инструментов управления инфраструктурой для автоматизации	K0 Знание инструментов автоматизации подготовки, тестирования и развертывания новой, измененной инфраструктуры K1 Знание стандартов и процедур для выявления операционных проблем и внесения своего вклада в их решение C1 Умение отслеживать безопасность и устойчивость систем и услуг

	предоставления, тестирования, развертывания и мониторинга компонентов инфраструктуры.	
21. Администрирование базы данных (Database administration) **DBAD**	Установка, настройка, обновление, администрирование, мониторинг и обслуживание баз данных. Обеспечение поддержки операционных баз данных в производственном использовании и для внутренних или промежуточных целей, таких как итерационные разработки и тестирование. Повышение производительности баз данных и инструментов и процессов для администрирования баз данных (включая автоматизацию).	K1 Знание процессов администрирования баз данных, включая автоматизацию C1 Умение использовать программное обеспечение и инструменты системы управления базами данных, а также знание логических схем баз данных для исследования проблем, сбора статистики производительности и создания отчетов C2 Умение выполнять настройку, установку и реконфигурацию базы данных и сопутствующих продуктов C3 Умение контролировать активность базы данных и использование ресурсов. C4 Умение оптимизировать производительность базы данных и планировать прогнозируемые потребности в ресурсах
22. Управление хранением (Storage management) **STMG**	Планирование, внедрение, настройка и настройка аппаратного и программного обеспечения хранения данных, охватывающего оперативное, автономное, удаленное и удаленное хранение данных (резервное копирование, архивирование и восстановление) и обеспечивающего соблюдение нормативных требований и требований безопасности.	K0 Знание нормативных требований и требований безопасности C1 Умение разрабатывать стратегии управления хранилищем и данными на основе уровня критичности информации C2 Умение создавать, совершенствовать и поддерживать ИТ-услуги с обеспечением безопасности данных, а также их целостности и доступности C3 Умение разрабатывать стандарты, процедуры и принципы для реализации функций защиты данных и аварийного восстановления C4 Умение использовать различные сетевые и автономные устройства хранения данных C5 Умение оценить операционные показатели для обеспечения корректирующего и упреждающего обслуживания систем хранения и резервного копирования в поддержку требований по защите деловой информации
23. Поддержка сети (Network support) **NTAS**	Предоставление услуг по обслуживанию и поддержке сети. Поддержка может	K1 Знание функциональности сети, правильной работы, ограничений, разработки

	предоставляться как пользователям систем, так и функциям доставки услуг. Поддержка обычно принимает форму исследования и решения проблем и предоставления информации о системах. Это может также включать мониторинг их работы. Проблемы могут быть решены путем предоставления рекомендаций или обучения пользователей о функциональных возможностях сети, правильной работе или ограничениях, путем разработки обходных путей, исправления ошибок или внесения общих или специфических для сайта изменений.	обходных путей, исправления ошибок или внесения общих или специфических для сайта изменений C1 Умение использовать программное обеспечение и инструменты сетевого управления для исследования и диагностики сетевых проблем, сбора статистики производительности и создания отчетов, работая с пользователями, другими сотрудниками и поставщиками по мере необходимости C2 Умение проводить исследование, диагностику и разрешение сетевых проблем.
24. Управление проблемами (Problem management) **PBMG**	Разрешение (как реактивных, так и проактивных) проблем на протяжении всего жизненного цикла информационной системы, включая классификацию, установление приоритетов и инициирование действий, документирование основных причин и реализацию мер по предотвращению будущих инцидентов.	K0 Знание мер прогнозирования, расследования и решения проблем систем и услуг K1 Знание мер правовой защиты C1 Умение разрабатывать решения проблем на протяжении жизненного цикла информационной системы
25. Управление объектами (Facilities management) **DCMA**	Планирование, контроль и управление всеми средствами, которые в совокупности составляют IT-инфраструктуру. Это включает обеспечение физической среды и управление ею, включая распределение пространства и мощности, а также мониторинг окружающей среды для предоставления статистики использования энергии. Охватывает контроль физического доступа и соблюдение всех обязательных правил и норм, касающихся здоровья и безопасности на работе.	K0 Знание стандартов, процессов и документации для центров обработки данных C1 Умение оптимизировать эффективность заполнения пространства дата-центра
26. Управление качеством (Quality management) **QUMG**	Управление качеством устанавливает внутри организации культуру качества и систему процессов и методов работы для достижения целей организации в области качества. Это включает в себя применение методов для мониторинга и улучшения качества любого аспекта функции, процессов, продуктов, услуг или данных. Достижение и поддержание соответствия национальным и	K1 Знание методов и стандартов менеджмента качества K2 Знание международных и национальных стандартов C1 Умение обеспечить требуемый организационный уровень качества проектов, команд и функций C2 Умение обеспечивать соответствие национальным и международным стандартам, в зависимости от обстоятельств C3 Умение определить степень

	международным стандартам, в зависимости от обстоятельств, и внутренней политики, в том числе касающейся качества, обслуживания, устойчивости и безопасности.	соответствия политики в области качества потребностям и целям организации
27. Сорсинг (Sourcing) **SORC**	Предоставление политики, внутренних стандартов и рекомендаций по закупке или вводу в эксплуатацию поставляемых и разработанных внутри компании продуктов и услуг. Обеспечение коммерческого управления, соответствия законодательству и обеспечение информационной безопасности. Внедрение процессов закупок, соответствующих требованиям, с полным учетом проблем и императивов как со стороны ввода в эксплуатацию, так и со стороны поставщика. Идентификация и управление поставщиками для обеспечения успешной доставки продуктов и услуг, необходимых бизнесу.	K1 Знание альтернативных моделей поиска поставщиков, а также по политику и процедуры, охватывающие отбор поставщиков, тендеры и закупки K2 Знание действующего законодательству и политики C1 Умение анализировать данные для поддержки сотрудничества и согласования условий, отражающих масштаб требований и способствующих хорошей работе C2 Умение выбрать эффективные стратегии управления взаимоотношениями с поставщиками, охватывающие эффективные операционные отношения на всех уровнях
28. Управление поставщиками (Supplier management) **SUPP**	Согласование целей и деятельности организации с поставщиками со стратегиями и планами поставщиков, балансировкой затрат, эффективности и качества обслуживания. Установление рабочих отношений, основанных на сотрудничестве, доверии и открытом общении, для поощрения совместных инноваций и улучшения обслуживания с поставщиками. Упреждающее вовлечение поставщиков для взаимной выгоды для разрешения операционных инцидентов, проблем, плохой работы и других источников конфликтов. Использование четких путей эскалации для обсуждения и решения проблем. Управление производительностью и рисками у нескольких поставщиков (внутренних и внешних) с использованием набора согласованных показателей.	K1 Знание стратегий управления поставщиками C1 Умение проводить мониторинг и оформлять отчеты о работе поставщиков, удовлетворенности клиентов и анализе рынка C2 Умение управлять поставщиками для достижения ключевых показателей эффективности и согласованных целевых показателей, операционными отношениями между поставщиками C3 Умение создавать среду, в которой организация и ее поставщики сотрудничают к их взаимной выгоде, обеспечивая развитие и поддержание позитивных и эффективных рабочих отношений по всей цепочке поставок C4 Умение управлять рисками, связанными с информационной безопасностью, непрерывностью и целостностью поставок
29. Консультация специалиста (Specialist advice) **TECH**	Разработка и использование экспертных знаний в любой конкретной области информационных или коммуникационных технологий, цифровой работы, конкретных методов, методологий,	K1 Знание границ собственных специальных знаний C1 Умение предоставить подробные и конкретные консультации относительно применения их специализации(специализаций) к

	продуктов или областей применения в целях предоставления консультаций специалистам.	планированию и операциям организации С2 Умение обеспечивать организационное руководство и руководящие принципы для содействия развитию и использованию специальных знаний в организации
30. Управление знаниями (Knowledge management) **KNOW**	Систематическое управление жизненно важными знаниями для создания ценности для организации путем сбора, обмена, развития и использования коллективных знаний организации для повышения эффективности работы, поддержки принятия решений и снижения рисков. Обеспечение доступа к неформальным, неявным знаниям, а также к формальным, документированным, явным знаниям путем содействия внутреннему и внешнему сотрудничеству и коммуникациям.	К1 Знание методов сбора, обмена, развития и использования коллективных знаний организации для повышения эффективности работы, поддержки принятия решений и снижения рисков К2 Знание передовых практических подходов к управлению информацией и знаниями, а также способов внедрить их во все области своей работы С1 Умение выбрать соответствующие методы и инструменты управления знаниями в соответствии с согласованной политикой и стандартами С2 Умение разрабатывать организационную политику, стандарты и руководящие принципы управления знаниями, которые позволяют организациям быстро реагировать, предоставлять услуги, принимать решения и предпринимать действия С3 Умение осуществлять мониторинг и оценку инициатив по обмену знаниями С4 Умение разработать общеорганизационную стратегию управления знаниями для сбора, систематизации и развития информации, знаний и историй от сотрудников, клиентов и внешних партнеров
31. Стратегическое планирование (Strategic planning) **ITSP**	Создание, повторение и поддержание стратегии с целью приведения организационных действий, планов и ресурсов в соответствие с бизнес-целями, а также разработка планов продвижения вперед и реализации этой стратегии. Работа с заинтересованными сторонами для коммуникации и внедрения стратегического управления с помощью целей, подотчетности и мониторинга прогресса.	С1 Умение установить политику, стандарты и руководящие принципы для характеристики того, как организация проводит разработку стратегии и планирование С2 Умение разработать, внедрить и проанализировать процессы, обеспечивающие включение стратегического управления в управленческие и оперативные планы организации С3 Умение создавать стратегии с целью приведения организационных действий, планов и ресурсов в соответствие с бизнес-целями

32. Управление активами (Asset management) **ASMG**	Управление жизненным циклом всех управляемых активов (аппаратное и программное обеспечение, интеллектуальная собственность, лицензии, гарантии и т. д.) включая безопасность, инвентаризацию, соответствие, использование и утилизацию, с целью защиты и защиты портфеля корпоративных активов, оптимизации общей стоимости владения и устойчивости за счет минимизации операционных затрат, улучшения инвестиционных решений и использования потенциальных возможностей. Использование международных стандартов для управления активами (аналогичных ISO серии 55000) и тесная интеграция со стандартами, связанными с безопасностью, изменениями и управлением конфигурациями (аналогичных ISO серии 61508) для улучшенной разработки управления активами.	K0 Знание основ куррикулума CSec2017 K1 Знание международных и национальных стандартов для управления активами (аналогичных ISO серии 55000) K2 Знание международных и национальных стандартов по функциональной безопасности систем (аналогичных ISO серии 61508) K3 Знание международных и национальных стандартов для управления рисками (аналогичных ISO серии ISO 31000) K4 Знание современных методов в области анализа рисков C1 Умение использовать на практике стандарты в области управления активами, оценки функциональной безопасности систем, управления рисками (аналогичных стандартам ISO серий 55000, 61508, 31000) C2 Умение применять современные методы в области анализа рисков на практике
33. Релиз и развертывание (Release and deployment) **RELM**	Применение процессов, систем и функций, необходимых для того, чтобы новые и измененные услуги и функции были доступны для использования. Деятельность может включать, но не ограничиваться: ▪ упаковка и развертывание изменений и обновлений программного обеспечения для выпуска в рабочую среду ▪ управление непрерывной доставкой/развертыванием с использованием средств автоматизации для контейнеризации и оркестровки ▪ использование средств управления пакетами или средств управления жизненным циклом приложений для контроля зависимостей, версий и библиотек программного	K1 Знание методов, процессов и средств автоматизации развертывания и выпуска релиза C1 Умение руководить оценкой, анализом, планированием пакетов релизов, учитывая оценку рисков

	обеспечения ▪ объединение изменений для формирования релиза, предоставляющего новую услугу или обновляющего существующую услугу ▪ соблюдение установленных стандартов безопасности, охраны и качества ▪ обеспечивая контролируемую и эффективную передачу оперативному руководству и сообществу пользователей.	
34. Контроль изменений (Change control) **CHMG**	Оценка рисков, связанных с предлагаемыми изменениями, и обеспечение контроля и координации изменений продуктов, услуг или систем. Контроль изменений применяется ко всему, что влияет на действующие продукты, услуги или системы. К ним обычно относятся - приложения, инфраструктура, документация, процессы, элементы конфигурации, поставщики. Деятельность может включать, но не ограничиваться: ▪ управление жизненным циклом запросов на изменения - регистрация, оценка, авторизация, планирование, развертывание ▪ оценка рисков и снижение рисков для доступности, производительности, безопасности и соответствия требованиям продуктов и услуг, на которые влияет изменение ▪ разработка процессов для стандартных, обычных или аварийных	K1 Знание инструментов, методов, процессов администрирования, отслеживания, регистрации и составления отчетов по запросам на изменения C1 Умение применить процедуры контроля изменений C2 Умение оценить, проанализировать, разработать и документировать изменения на основе запросов на изменения C3 Умение разработать и настроить инструменты управления и отчетности по жизненному циклу запросов на изменения C4 Умение выявить проблемы в процессе жизненного цикла запросов на изменения

	изменений ▪ разработка методов и инструментов для автоматизации процессов управления изменениями с целью обеспечения непрерывной интеграции.	
35. Управление непрерывностью (Continuity management) **COPL**	Обеспечение непрерывности обслуживания планирование и поддержка, как часть или в тесном сотрудничестве с функцией, которая планирует непрерывность бизнеса для всей организации. Идентификация информационных систем, поддерживающих критически важные бизнес-процессы. Оценка рисков для доступности, целостности и конфиденциальности критически важных систем. Координация процедур планирования, проектирования, тестирования и технического обслуживания, а также планов действий в чрезвычайных ситуациях для устранения рисков и поддержания согласованных уровней непрерывности.	K0 Знание информационно-коммуникационных систем, поддерживающих важнейшие процессы K1 Знание рисков, связанных с функционированием систем K2 Знание стратегий тестирования планов и процедур обеспечения непрерывности для учета подверженности риску C1 Умение оценивать риски доступности, целостности и конфиденциальности систем, поддерживающих критически важные процессы C2 Умение планировать, проектировать и тестировать процедуры технического обслуживания C3 Умение планировать, проектировать и тестировать планы действий в чрезвычайных ситуациях
36. Управление информацией (Information management) **IRMG**	Общее управление тем, как все виды информации, структурированной и неструктурированной, независимо от того, производится ли она внутри или снаружи, используются для поддержки принятия решений, бизнес-процессов и цифровых услуг. Включает разработку и продвижение стратегии и политики, охватывающих разработку информационных структур и таксономий, разработку политики поиска и содержания данных, а также разработку политики, процедур, методов работы и подготовки кадров для содействия соблюдению законодательства, регулирующего все аспекты хранения, использования и раскрытия данных.	K0 Знание механизмов контроля за внутренним делегированием полномочий, аудитом и контролем, связанными с управлением информацией и документацией K1 Знание нормативных актов, стандартов и кодексов надлежащей практики, касающихся информации и документации, делопроизводства, обеспечения информационной безопасности и защиты данных C1 Умение оценивать и управлять рисками, связанными с использованием информации C2 Умение создавать и вести инвентаризацию информационных активов, на которые распространяется действие законодательства C3 Умение воспринимать и

		анализировать информацию внутренних и внешних систем и источников С4 Умение разрабатывать стратегии соблюдения внутренних и внешних нормативных актов, относящихся к использованию информации