НЕКОММЕРЧЕСКОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО

«КАРАГАНДИНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ИМЕНИ АБЫЛКАСА САГИНОВА»

«Утверждаю»

Член Правления – Проректор

по академическим вопросам

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.М. Темербаева

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г.

**РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА (SYLLABUS)**

Дисциплина SSSIB 2301 Сертификация и стандартизация средств информационной безопасности

Модуль PO 08 Профессионально-ориентированный 1

Образовательная программа 6В06301 «Системы информационной

безопасности»

Разработал \_\_\_\_\_\_\_\_\_\_\_ Солодовникова И.В. «\_\_\_»\_\_\_\_\_\_\_\_\_2023 г.

(подпись) (ФИО)

Обсуждена на заседании кафедры «Информационные технологии и безопасность»

Протокол № \_\_\_\_\_\_\_ от «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_2023 г.

Зав. кафедрой \_\_\_\_\_\_\_\_\_\_\_ Коккоз М.М. «\_\_\_»\_\_\_\_\_\_\_\_\_2023г.

(подпись) (ФИО)

Одобрена Комитетом по обеспечению качества факультет инновационных технологий

Протокол № \_\_\_\_\_\_\_\_ от «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2023 г.

Председатель \_\_\_\_\_\_\_\_\_\_\_ Тау А.Ғ. «\_\_\_»\_\_\_\_\_\_\_\_\_2023 г.

(подпись) (ФИО)

2023

**1 Сведения о преподавателе и контактная информация**

Ф.И.О. Солодовникова Ирина Валентиновна

Ученая степень, звание, должность старший преподаватель

Кафедра «Информационные технологии и безопасность» находится в главном корпусе (пр. Нурсултана Назарбаева, 56), аудитория 428, контактный телефон 56-59-35 доб. 1028, e-mail itb\_kargtu@kstu.kz.

**2 Трудоемкость дисциплины**

| Форма  обучения | Семестр | Количество  кредитов | Лекции | Практические работы | Лабораторные работы | Экзамен | СРСП, часов | Количество контактных  часов | СРС | Итого, часов |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| очная | 3 | 5 | 15 | - | 30 | 5 | 15 | 65 | 85 | 150 |
| очная на базе ТиПО | 3 | 5 | 15 | - | 30 | 5 | 15 | 65 | 85 | 150 |

**3 Характеристика дисциплины**

Дисциплина «Сертификация и стандартизация средств информационной безопасности» входит в вузовский компонент цикла профилирующих дисциплин.

**4 Цель изучения дисциплины**

Дисциплина «Сертификация и стандартизация средств информационной безопасности» ставит целью ознакомление студентов с правовыми и организационными основами в области стандартизации и сертификации средств защиты информации, формирование навыков практического применения полученных знаний в профессиональной деятельности.

**5 Задачи дисциплины**

Задачи дисциплины следующие:

* изучить цели и задачи государственного регулирования в области и стандартизации и подтверждения соответствия;
* изучить и систематизировать требования национальных и международных стандартов в сфере информационной безопасности;
* развить навыки работы с нормативными документами по техническому нормированию и стандартизации, подтверждению соответствия;
* изучить цели, принципы, формы подтверждения соответствия, правил сертификации продукции и организации работ;
* приобрести навыки организации и проведения процедур подтверждения соответствия.

**6 Результаты изучения дисциплины**

После изучения данной дисциплины ожидается, что обучающийся:

6.1 Эксплуатирует программно-аппаратные средства защиты информации:

6.1.1 координирует работу по разработке (актуализации) документов, регламентирующих процессы обеспечения ИБ (регистрация и учет событий ИБ, резервное копирование, антивирусная защита, контроль доступа, обеспечение ИБ при работе со съемными носителями, мобильными устройствами, почтовыми службами и Интернетом, управление лицензиями и версионностью ПО);

6.2 организовывает процесс защиты информации:

6.2.1 осуществляет анализ, выбор методик и методов оценки и реализации процессов управления ИБ охватывающие процессы управления рисками, активами, инцидентами, техническими уязвимостями, угрозами;

6.2.2 координирует деятельность по разработке (актуализации) политики ИБ, процессов управления ИБ и документов, регламентирующих процессы обеспечения ИБ;

6.2.3 использует нормативно-правовые документы Республики Казахстан при проектировании, эксплуатации и обслуживании объектов профессиональной деятельности;

6.3 знает основные термины и определения в области сертификации;

6.4 умеет применять стандарты в сфере защиты информации для решения задач сертификации средств информационной безопасности;

6.5 умеет выбирать схемы подтверждения соответствия, формировать комплект документов, необходимых для прохождения процедур подтверждения соответствия;

6.6 анализирует проекты стандартов на соответствие действующим законодательным актам в области информационной безопасности, а также современному состоянию и перспективам развития науки и техники.

**7 Пререквизиты**

Для изучения данной дисциплины необходимо усвоение следующих дисциплин: «Информационно-коммуникационные технологии».

**8 Постреквизиты**

Знания, полученные при изучении дисциплины «Сертификация и стандартизация средств информационной безопасности» используются при освоении следующих дисциплин: «Организационно-правовое обеспечение информационной безопасности», «Менеджмент информационной безопасности», «Проектирование систем защиты информации».

**9** **Тематический план дисциплины**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Наименование раздела, (темы) | Трудоемкость по видам занятий, ч. | | | | | |
| лекции | семинар | лабора-торные | СРСП | СРС |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1. Стандартизация, сертификация, аккредитация, лицензирование и разрешения в сфере обеспечения ИБ. Законы РК «О стандартизации», «О техническом регулировании», «О разрешениях и уведомлениях», «Об информатизации». Постановление Правительства РК «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности». | 3 |  |  | 3 | 5 |
| 2. Анализ предметной области и определение требований к ИС. СТ РК 1090-2002 «Спецификация требований к программному обеспечению». IEEE 830-1998 «Методика составления спецификаций требований к программному обеспечению, рекомендуемая IEEE», открытый стандарт UML в анализе и проектировании программных систем. СТ РК 34.015-2002 Техническое задание на создание автоматизированной системы. Приказ «Об утверждении Правил классификации объектов информатизации и классификатор объектов информатизации», комплект документов, необходимых для прохождения процедур подтверждения соответствия. | 3 |  |  | 3 | 5 |
| 3. Управление рисками ИБ. Выявление требований к ИБ. Риск-ориентированный подход. Постановление Правительства Республики Казахстан «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»; СТ РК ИСО/МЭК 31010 «Менеджмент риска. Методы оценки рисков»; СТ РК ИСО/МЭК 27005 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности»; Формирование каталога угроз (рисков) ИБ; Методика оценки рисков; Разработка плана обработки угроз | 3 |  |  | 3 | 5 |
| 4. Стандарты ИБ серия 27000. СТ РК ISO/IEC 27000 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь. СТ РК ISO/IEC 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования. СТ РК ISO/IEC 27002 Информационная технология Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации. Меры защиты согласно СТ РК ISO/IEC 27002. СТ РК ISO/IEC 27003 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности. СТ РК ISO/IEC 27004 Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерение. | 3 |  |  | 3 | 5 |
| 5. Технология сертификации средств ИБ. Проведение испытаний объектов информатизации на соответствие требованиям информационной безопасности. Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности РК «Об утверждении методики и правил проведения испытаний объектов информатизации "электронного правительства" и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности». Порядок и схемы проведения сертификации.СТ РК ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Часть 2. Функциональные требования безопасности Часть 3. Требования к обеспечению защиты»;Оценочный уровень доверия.Реестр доверенного программного обеспечения и продукции электронной промышленности. | 3 |  |  | 3 | 5 |
| 6. Международные стандарты информационной безопасности. |  |  | 4 |  | 10 |
| 7. Анализ предметной области. Предварительное обследование. |  |  | 4 |  | 10 |
| 8. Разработка, тестирование и спецификация требований к информационной системе |  |  | 6 |  | 10 |
| 9. Разработка технического задания |  |  | 6 |  | 10 |
| 10. Методология анализа защищенности информационной системы |  |  | 6 |  | 10 |
| 11. Технология сертификации средств защиты информации |  |  | 4 |  | 10 |
| **ИТОГО:** | **15** | **-** | **30** | **15** | **85** |

**10 Перечень семинаров**

Не предусмотрено рабочим учебным планом.

**11 Перечень лабораторных работ**

| Наименование лабораторной работы | Количество часов |
| --- | --- |
| Международные стандарты информационной безопасности. | 4 |
| Анализ предметной области. Предварительное обследование. | 4 |
| Разработка, тестирование и спецификация требований к информационной системе | 6 |
| Разработка технического задания | 6 |
| Методология анализа защищенности информационной системы | 6 |
| Технология сертификации средств защиты информации | 4 |
| Итого | 30 |

**12 Тематика курсового проекта**

Не предусмотрено рабочим учебным планом.

**13 Темы контрольных заданий для СРС**

**13.1 Творческие и исследовательские задания**

1. Проанализировать Казахстанское и зарубежное законодательство в области ИБ.
2. Составить глоссарий терминов.
3. Рассмотреть международные и национальные стандарты и спецификации в области ИБ.
4. Рассмотреть организационную структуру технического задания АС
5. Рассчитать класс ИС.
6. Рассмотреть сертификацию в области ИБ.
7. Проанализировать порядок разработки стандартов.
8. Проанализировать деятельность ИСО в области сертификации.

**13.2 Контрольные вопросы для СРС**

1. Какие нормативные документы существуют в области стандартизации?

2. Что такое объект стандартизации?

3. Что является результатом этапа системного анализа предметной области?

4. Назовите известные вам способы извлечения требований.

5. Какие требования считаются модифицируемыми?

6. Какие требования считаются корректными?

7. К какому стандарту относится модель вариантов использования?

8. Для чего разрабатывается спецификация вариантов использования?

9. Какие допущения регламентирует СТ РК при написании ТЗ?

10. В каком разделе указывают требования к процессам верификации, аттестации, совместной проверки, аудита?

11. Что принято называть угрозой информационной безопасности?

12. Какова классификация угроз информационной безопасности?

13. Какие основополагающие документы используются в области информационной безопасности?

14. Что понимают под сертификацией?

15. Основные отличия сертификации от лицензирования и аттестации.

**14 Тематический план самостоятельной работы студента с преподавателем**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование темы СРСП | Цель занятия | Форма проведения занятия | Содержание  задания | Рекомендуемая литература |
| Стандартизация, сертификация, аккредитация, лицензирование и разрешения в сфере обеспечения ИБ. | Систематизация и закрепление знаний | Конференция | 1. Подготовить доклад  2. Выполнить задание СРС 13.1.1 | [1-6]  Конспект лекций. |
| Анализ предметной области и определение требований к ИС. | Исследовать предметную область и составить спецификацию ИС | Индивидуальное консультирование по заданию | 1. Изучить и проанализировать теоретический материал, ответить на контрольные вопросы.  2. Выполнить задание СРС 13.1.2, 13.1.3, 13.1.4 | [7-10,20]  Конспект лекций. |
| Управление рисками ИБ. Выявление требований к ИБ. Риск-ориентированный подход. | Исследовать предметную область и составить каталог угроз (рисков) ИБ; выполнить оценку рисков; разработать план обработки угроз | Индивидуальное консультирование по заданию | 1. Изучить и проанализировать теоретический материал, ответить на контрольные вопросы.  2. Выполнить задание СРС 13.1.5 | [11, 12]  Конспект лекций. |
| Стандарты ИБ серия 27000 | Исследовать предметную область и составить реестр документов по стандартизации | Индивидуальное консультирование по заданию | 1. Изучить и проанализировать теоретический материал, ответить на контрольные вопросы.  2. Выполнить задание СРС 13.1.7 | [13- 17]  Конспект лекций. |
| Технология сертификации средств ИБ. Проведение испытаний объектов информатизации на соответствие требованиям информационной безопасности. | Исследовать предметную область и составить перечень национальных стандартов | Индивидуальное консультирование по заданию | 1. Изучить и проанализировать теоретический материал, ответить на контрольные вопросы.  2. Выполнить задание СРС 13.1.6, 13.1.8 | [18, 19]  Конспект лекций. |

**15 Критерии и политика оценивания**

15.1 Шкала оценивания

|  |  |  |
| --- | --- | --- |
| Оценка | Цифровой эквивалент | Баллы (%-ное содержание) |
| А | 4,0 | 95-100 |
| А- | 3,67 | 90-94 |
| В+ | 3,33 | 85-89 |
| В | 3,0 | 80-84 |
| В- | 2,67 | 75-79 |
| С+ | 2,33 | 70-74 |
| С | 2,0 | 65-69 |
| С- | 1,67 | 60-64 |
| D+ | 1,33 | 55-59 |
| D | 1,0 | 50-54 |
| FX | 0,5 | 25-49 |
| F | 0 | 0-24 |

15.2 Итоговая оценка по дисциплине определяется как сумма максимальных показателей успеваемости по рубежным контролям (до 60%) и промежуточной аттестации (экзамен) (до 40%) и составляет значение до 100%.

| Виды работ | Академический период обучения, неделя | | | | | | | | | | | | | | | | | Итого, %  1РК  +2РК |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Сумма РК1 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | Сумма РК2 |
| Лекции (посещаемость) | 1 |  | 1 |  | 1 |  | 1 |  | 4 | 1 |  | 1 |  | 1 |  | 1 | 4 | 8 |
| Лаб. работы |  | 20 |  | 20 |  |  | 20 |  | 60 |  | 20 |  |  | 20 |  | 20 | 60 | 120 |
| Модуль |  |  |  |  |  |  |  | 20 | 20 |  |  |  |  |  |  | 20 | 20 | 40 |
| СРСП, СРС |  |  | 5 |  | 5 |  |  | 6 | 16 |  | 5 |  | 5 |  |  | 6 | 16 | 32 |
| Итого по РК |  |  |  |  |  |  |  |  | 100 |  |  |  |  |  |  |  | 100 | 200 |
| Сумма показателей по РК |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 60 |
| Экзамен |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 40 |
| Итого |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 100 |

15.3 Политика оценивания

15.3.1 Лабораторные работы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Критерий | Удельный вес | Комментарий | Рекомендации по совершенствованию работы |
| 1 | Программная реализация задачи согласно варианту | 50% | Оценивается правильность и оптимальность решения |  |
| 2 | Срок сдачи | 20% | Оценивается срок сдачи – в срок/ с опозданием |  |
| 3 | Защита работы, ответы на контрольные вопросы | 30% | Оцениваются знания и навыки в области алгоритмов и структур данных |  |

15.3.2 СРСП+СРС

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Критерий оценивания | Удельный вес | Комментарий | Рекомендации по совершенствованию работы |
| 1 | Разработка алгоритмов и программ | 75% | Оценивается разработка алгоритмических и программных решений |  |
| 2 | Срок сдачи | 10% | Оценивается срок сдачи – в срок/ с опозданием |  |
| 3 | Выполнение заданий СРС | 15% | Оценивается оптимальность решения |  |

15.3.3 Модуль

Результаты тестирования генерируются автоматически в зависимости от количества тестовых заданий.

**16 График выполнения и сдачи заданий по дисциплине**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Виды работ | № темы (лекции, лабораторной, практической работы, семинара).  Цель и содержание задания | Рекомендуемая литература | Форма отчетности | Вид контроля | Срок сдачи | Баллы за выполненную работу | Ожидаемые  результаты |
| Посещаемость лекций | № 1-5 (Усвоение материала по темам) | [1..20],  Конспекты лекций | Отметка в журнале посещений | текущий | На каждой лекции | 8 | 6.1-6.5 |
| Лаб. работы | № 6  Изучить основные направления обеспечения ИБ как составляющей национальной безопасности в ведущих зарубежных странах. | МУ к ЛР | Отчет по лабораторной работе | текущий | 3 неделя | 20 | 6.3-6.6 |
| Лаб. работы | № 7  Изучить принципы первичного обследования и анализа предметной области, выполнить анализ полученного материала, разработать внешнее описание системы. | [7-10, 20]  МУ к ЛР  Конспекты лекций | Отчет по лабораторной работе | текущий | 6 неделя | 20 | 6.3-6.6 |
| Лаб. работы | № 8  Изучить критерии качества требований, научиться создавать формальные модели и на их основе определять спецификации. | [7-10, 20]  МУ к ЛР  Конспекты лекций | Отчет по лабораторной работе | текущий | 8 неделя | 20 | 6.3-6.6 |
| Лаб. работы | № 9  Сформировать навыки разработки и оформления технического задания в соответствии с СТ РК 34.015. | [7-10, 20]  МУ к ЛР  Конспекты лекций | Отчет по лабораторной работе | текущий | 10 неделя | 20 | 6.3-6.6 |
| Лаб. работы | № 10  Выявление значимых составляющих ИБ и характеристик ИС, выполнить оценку защищенности ИС. | [13-17]  МУ к ЛР  Конспекты лекций | Отчет по лабораторной работе | текущий | 13 неделя | 20 | 6.3-6.6 |
| Лаб. работы | № 11  Изучение методики и правил проведения испытаний объектов информатизации на соответствие требованиям ИБ. | [18-19]  МУ к ЛР  Конспекты лекций | Отчет по лабораторной работе | текущий | 15 неделя | 20 | 6.3-6.6 |
| СРСП+СРС | №1-2 (Получение практических навыков) *см.* *п. 14* | [1..12,20] | Выполнение индивидуальных заданий | текущий | 3,5,8 неделя | 16 | 6.1-6.4 |
| СРСП+СРС | №3-5 (Получение практических навыков) *см.* *п. 14* | [13..19] | Выполнение индивидуальных заданий | текущий | 10,12,15 неделя | 16 | 6.1-6.4 |
| Модуль | Оценка текущего уровня знаний студентов | [1..20]  МУ к ЛР  Конспекты лекций | Письменный опрос в форме тестовых заданий. | текущий | 8 неделя | 20 | 6.1-6.5 |
| Модуль | Оценка текущего уровня знаний студентов | [1..20]  МУ к ЛР  Конспекты лекций | Письменный опрос в форме тестовых заданий. | текущий | 15 неделя | 20 | 6.1-6.5 |
| Сумма показателей по РК |  |  |  |  |  | 200/2=100 |  |
| Экзамен | Проверка усвоения материала дисциплины | [1..20]  Конспекты лекций | Письменный экзамен | итоговый | В период сессии | 40 | 6.1-6.6 |
| Итого |  |  |  |  |  | 100 |  |

**17 Политика и процедуры курса**

При изучении дисциплины «Сертификация и стандартизация средств информационной безопасности» прошу соблюдать следующие правила:

17.1 Не опаздывать на занятия.

17.2 Не пропускать занятия без уважительной причины, в случае болезни прошу представить справку, в других случаях – объяснительную записку.

17.3 В обязанности студента входит посещение всех видов занятий.

17.4 Согласно календарному графику учебного процесса сдавать все виды контроля.

17.5 Пропущенные лабораторные занятия отрабатывать в указанное преподавателем время.

17.6 При выполнении всех видов работ ссылаться на п.15.3.

**18 Академическая честность**

18.1 В соответствии с Антикоррупционным стандартом КарТУ академическая добропорядочность – это постоянное обязательство участников образовательного процесса и образовательных учреждений действовать согласно ценностям и принципам, исключающим коррупционные риски и проявления, формирующим и укрепляющим профессиональную среду, позволяющую им придерживаться такого поведения.

18.2 Продвижение и защита академической честности являются результатом взаимных усилий всех обучающихся и сотрудников КарТУ.

18.3 Обучающиеся обязаны добросовестно соблюдать принципы академической честности.

18.4 Согласно Кодексу чести студентов, магистрантов и докторантов КарТУ (Кодекс) академическое нарушение (академическая недобропорядочность) представляет собой действие, когда обучающийся:

а) пытается присвоить себе заслуги за работу или усилия другого человека без получения разрешения или, не ссылаясь на его работы («плагиат»);

б) использует несанкционированные материалы или ложные данные при выполнении учебных заданий;

в) подделывает или фальсифицирует академические документы или ведомости успеваемости;

г) умышленно препятствует академической работе других обучающихся или подрывает ее;

д) совершает действия, направленные на представление ложной информации;

е) занимается списыванием в любой форме на экзамене или во время НАО «Карагандинский технический университет» Правила Оформления учебно-методического комплекса ПР КарТУ IV – 01-2021 Версия 02 Дата 2021.10.05 Стр. 18 из 27 Запрещается несанкционированное копирование документа выполнения заданий;

ж) содействует другим обучающимся в совершении какого-либо из описанных деяний.

18.5 Кодексом определены меры ответственности обучающегося за академические нарушения:

* устное предупреждение;
* аннулирование работы и/или выставленной оценки;
* недопуск к защите оцениваемых работ, в т.ч. диссертационных работ;
* отчисление из КарТУ.

Список литературы

1 Закон РК «О стандартизации» от 5 октября 2018 года № 183-VІ ЗРК

2 Закон РК «О техническом регулировании» от 30 декабря 2020 года № 396-VI ЗРК

3 Постановление Правительства РК «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» от 20 декабря 2016 года № 832

4 Закон РК «О разрешениях и уведомлениях» от 16 мая 2014 года № 202-V ЗРК

5 Закон РК «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК

6 Стандарт организации ПР V-08-2022 Общие требования к оформлению текстовых учебных документов и основных надписей

7 Стандарт IEEE 830-1998 «Методика составления спецификаций требований к программному обеспечению, рекомендуемая IEEE»

8 СТ РК 1090-2002 ЕСПД. «Спецификация требований к программному обеспечению».

9 СТ РК 34.015-2002 Техническое задание на создание автоматизированной системы

10 Приказ «Об утверждении Правил классификации объектов информатизации и классификатор объектов информатизации» и.о. Министра по инвестициям и развитию РК от 28 января 2016 года № 135

11 СТ РК ISO/IEC 27005-2013 Информационные технологии Методы обеспечения безопасности. Менеджмент риска информационной безопасности

12 СТ РК ISO/IEC 31010-2020 Менеджмент риска. Методы оценки риска

13 СТ РК ISO/IEC 27000-2019 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь

14 СТ РК ISO/IEC 27001-2015 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования

15 СТ РК ISO/IEC 27002-2015 Информационная технология Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации

16 СТ РК ISO/IEC 27003-2018 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности

17 СТ РК ISO/IEC 27004-2018 Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерение.

18 Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 года № 111/НҚ «Об утверждении методики и правил проведения испытаний объектов информатизации "электронного правительства" и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности».

19 Богульская, Н. А. Модели безопасности компьютерных систем: учебное пособие / Н. А. Богульская, М. М. Кучеров. — Красноярск: Сибирский федеральный университет, 2019. — 206 c.

20 Буч Г., Рамбо Д., Якобсон И. Язык UML. Руководство пользователя. 2-е изд.: Пер. с англ –М.: ДМК Пресс, 2014 – 496 с.