НЕКОММЕРЧЕСКОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО

«КАРАГАНДИНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ИМЕНИ АБЫЛКАСА САГИНОВА»

Кафедра ИТБ

СОЛОДОВНИКОВА И.В.

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

для проведения самостоятельной работы студента/

самостоятельной работы студента с преподавателем

Дисциплина **«**Сертификация и стандартизация средств информационной безопасности»

Модуль **«**Профессионально-ориентированный 1»

Образовательная программа 6B06301 – Системы информационной безопасности

Обсуждены на заседании кафедры «Информационные технологии и безопасность»

Протокол № 20а от «14» 05 2024г.

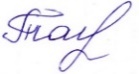


Зав. кафедрой \_\_\_\_\_\_\_\_\_\_ Коккоз М.М. «14» 05 2024г.

Одобрены Комитетом по обеспечению качества факультета инновационных

технологий

Протокол № 7 от «21» 05 2024г.



Председатель \_\_\_\_\_\_\_\_\_\_ Тау А.Ғ. «21» 05 2024г.

Караганда 2024

**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. |

**Темы контрольных заданий для СРС**

**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.

**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.

**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.