НЕКОММЕРЧЕСКОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО

«КАРАГАНДИНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ИМЕНИ АБЫЛКАСА САГИНОВА»

Кафедра ИТБ

СОЛОДОВНИКОВА И.В.

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

для выполнения лабораторных работ

по дисциплине

SSSIB 2301 Сертификация и стандартизация

средств информационной безопасности

Модуль PO 08 Профессионально-ориентированный 1

Образовательная программа 6B06301 – Системы информационной безопасности

Обсуждены на заседании кафедры «Информационные технологии и безопасность»

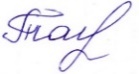
Протокол № 20а от «14» 05 2024г.



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

**Лабораторная работа № 1 (4 часа)**

**Международные стандарты информационной безопасности**

Цель работы: изучить основные направления обеспечения информационной безопасности как составляющей национальной безопасности в ведущих зарубежных странах, изучить основные документы, определяющих политику государства в области национальной безопасности

Методы исследования: теоретическое исследование (поиск, сбор, группировка и анализ информации по теме работы).

Задачи:

1. Изучить основные документы, определяющие политику государства в области национальной безопасности, следующих стран:

a. Стран Европейского союза.

b. США.

с. Китая.

d. РФ.

2. На основании каждого из приведённых документов определить:

a. угрозы безопасности, существующие на уровне страны или нации (объекты и угрозы информационной войны);

b. источники угроз (внешние и внутренние);

c. национальные интересы (в том числе их основные составляющие) и угрозы информационной безопасности в информационной сфере;

d. основные направления обеспечения информационной безопасности государства, в том числе технических объектов информационной сферы государства.

3. Произвести сравнение и анализ указанных выше документов между собой и с Концепцией цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности РК. Выявить общие черты и отличия.

Содержание отчета, оформленного в соответствии с требованиями ПР V-08-2022 Общие требования к оформлению текстовых учебных документов и основных надписей:

1. Перечень проанализированных документов, определяющих политику и стратегию государств в области национальной и информационной безопасности.

2. Выявленные угрозы информационной и кибербезопасности, существующие на уровне страны или нации. Приводится для каждого государства.

3. Выявленные источники угроз (внешние и внутренние). Приводится для каждого государства.

4. Национальные интересы и угрозы информационной безопасности в информационной сфере. Приводится для каждого государства.

5. Результаты сравнения (по пунктам 1–4) и анализа (в табличной форме) документов, определяющих политику и стратегию государств в области национальной и информационной безопасности.

6. Перечень использованных информационных источников.

Контрольные вопросы:

1. Какие нормативные документы существуют в области стандартизации?

2. Что такое объект стандартизации?

3. Какие виды стандартов Вы знаете?

4. Что такое стандартизация?

5. В каких формах может быть представлена информация?

6. Какая информация является документированной?

7. Что относится к информации ограниченного доступа?

8. Что понимается под защитой информации?

9. Что относится к основным характеристикам защищаемой информации?

10. Что такое угроза безопасности информации?

Список литературы

1. Постановление Правительства Республики Казахстан от 30 декабря 2021 года № 961 «Об утверждении Концепции развития отрасли информационно-коммуникационных технологий и цифровой сферы» // https://adilet.zan.kz/rus/docs/P2100000961 (Дата обращения: 18.02.2022).

2. Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации» // https://adilet.zan.kz/rus/docs/Z1500000418 (Дата обращения: 18.02.2022).

3. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» // https://adilet.zan.kz/rus/docs/Z1300000094 (Дата обращения: 18.02.2022).

4. Закон Республики Казахстан от 5 июля 2004 года № 567 «О связи» // https://adilet.zan.kz/rus/docs/Z040000567 (Дата обращения: 18.02.2022).

5. Закон Республики Казахстан от 7 января 2003 года № 370 «Об электронном документе и электронной цифровой подписи» // https://adilet.zan.kz/rus/docs/Z030000370 (Дата обращения: 18.02.2022).

6. Закон Республики Казахстан от 16 ноября 2015 года № 401-V ЗРК «О доступе к информации» // https://adilet.zan.kz/rus/docs/Z1500000401/z150401.htm (Дата обращения: 18.02.2022).

7. Указ Президента Республики Казахстан от 15 октября 2021 года № 674 «Об утверждении Концепции правовой политики Республики Казахстан до 2030 года» // https://adilet.zan.kz/rus/docs/U2100000674 (Дата обращения: 18.02.2022).

8. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»)» // https://adilet.zan.kz/rus/docs/P1700000407 (Дата обращения: 18.02.2022).

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

Лабораторная работа № 2 (4 часа)

Анализ предметной области. Предварительное обследование

Цель работы: изучение принципов первичного обследования и анализа предметной области, идентификация заинтересованных лиц и интервью с ними, анализ полученного материала, формулирование проблемы, ее актуальности и потребностей заинтересованных лиц.

Форма выполнения: беседа с заказчиком (в роли заказчика – преподаватель).

Задачи:

Ознакомиться с предметной областью по теме работы.

Выяснить субъективные цели и задачи (желаемый результат) у заказчика.

Провести анализ полученных данных.

Написать отчет о предварительном обследовании предметной области.

Требования и условия:

беседа проводится только в форме «вопрос-ответ»;

отчет сдается в печатной форме (объем 2-3 страницы);

исполнитель работы считается экспертом в предметной области, т.е. должен иметь достаточно глубокие познания, чтобы компетентно задавать вопросы.

Перед выполнением беседы с заказчиком заранее подготовить вопросы о требуемой программной системе.

Вопросы следует задавать в доступной непрофессионалу в области информационных технологий форме, избегая специальных и технических терминов.

При проведении беседы предпочтительно вести пометки или записи.

Протокол беседы необходимо в полном виде представить в отчете.

Порядок проведения работы:

1. Провести предварительный анализ задачи.

2. Составить перечень заинтересованных лиц – в произвольной форме.

3. Провести интервью и/или анкетирование с каждым заинтересованным лицом – в произвольной форме.

4. Составить словарь предметной области (глоссарий).

5. Подготовить документ «Обзор продукта».

Документ «Обзор продукта»

Другие названия документа: Описание постановки задачи. Внешнее описание системы. Vision.

Содержание:

(1) документ, составленный на основании пожеланий заказчика, достаточно точно определяющий задачи разработчиков ПС

(2) постановка задачи, решение которой должно обеспечить разрабатываемое ПС

(3) уместно привести качественную оценку необходимости (целесообразности), осуществимости разработки.

Контрольные вопросы:

1. Что является исходными данными для анализа проблемы (предметной области)?

2. Что является результатом этапа системного анализа предметной области?

3. Как определить заинтересованных лиц?

4. Какой на Ваш взгляд метод сбора информации наиболее эффективен? Обоснуйте.

5. Для чего проводятся интервьюирование и анкетирование?

6. Назовите известные вам способы извлечения требований.

Индивидуальные задания:

1. Информационная система гостиничного обслуживания.

2. Информационная система библиотеки.

3. Информационная система поликлиники.

4. Информационная система деканата.

5. Информационная система склада.

6. Информационная система учета рабочего времени.

7. Информационная система жилищного агентства.

8. Информационная система продажи билетов (кино, театры, концерты и т.д.)

9. Информационная система больницы

10. Информационная система для call-центра банка

11. Информационная система организации и ведения спортивных мероприятий (чемпионатов, турниров, игр и т.д.)

12. Информационная система построения расписания занятий

13. Информационная система оказания услуг по автоперевозкам (пассажирским и/или грузовым)

Рекомендуемая литература

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

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

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

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

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

Лабораторная работа № 3 (6 часов)

Разработка, тестирование и спецификация требований к информационной системе

Цель работы: составить и проанализировать требования к информационной системе, изучить критерии качества требований, научиться создавать формальные модели и на их основе определять спецификации разрабатываемого программного обеспечения, выполнить тестирование спецификации требований, оформить спецификации требований к программному обеспечению.

Задачи

1. Ознакомиться с процедурой разработки спецификации требований с применением Стандарта IEEE 830-1998 «Методика составления спецификаций требований к программному обеспечению, рекомендуемая IEEE» и СТ РК 1090-2002 ЕСПД. «Спецификация требований к программному обеспечению».

2. На основе предварительного анализа задачи, выполненного в лабораторной работе № 2, составить спецификацию функциональных требований. Для этого необходимо выполнить следующие задания:

— Идентифицировать действующих лиц системы.

— Идентифицировать варианты использования системы.

— Определить отношения между действующими лицами и вариантами использования.

— Составить полную диаграмму (или несколько диаграмм) использования.

— Определить, какие из вариантов использования (не менее трех) будут уточняться при последующем моделировании и будут реализованы в прототипе.

— Реализовать выбранные варианты использования в виде записи сценария на псевдокоде или на естественном языке.

3. Определить нефункциональные и специальные требования, если они необходимы, и объединить все требования в единый документ (текстовый документ с диаграммами использования, защищаемый артефакт).

Порядок выполнения работы

1. Изучить предлагаемый теоретический материал и стандарты IEEE 830, СТ РК 1090.

2. Составить информационную модель будущей системы, включающую в себя описание основных объектов системы и взаимодействия между ними. На основании полученной информационной модели и диаграмм использования сформировать требования пользователя и системные требования.

3. Провести тестирование требований, указать какие типы проверок выбрали.

4. Построить отчёт, включающий все полученные уровни модели, описание функциональных блоков, потоков данных, хранилищ и внешних объектов.

Контрольные вопросы:

1. Дайте определение понятию «требование».

2. Перечислите значения требований.

3. Какие бывают уровни представления требований?

4. К какому стандарту относится модель вариантов использования?

5. Что такое вариант использования?

6. Назовите элементы описания «Вариантов использования».

7. Какие вы знаете отношения между вариантами использования?

8. Что называют альтернативными или вторичными сценариями?

9. Опишите структуру спецификации варианта использования.

10. Для чего разрабатывается спецификация вариантов использования?

Рекомендуемая литература

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

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

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

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

Лабораторная работа № 4 (6 часов)

Разработка технического задания

Цель работы: Цель работы – сформировать навыки разработки и оформления технического задания в соответствии с СТ РК 34.015-2002 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

Задачи

1. Ознакомиться с процедурой разработки технического задания с применением СТ РК 34.015-2002.

2. На основе предварительного анализа задачи, выполненного в лабораторных работах № 2,3, написать разделы ТЗ и оформить его в соответствии с СТ РК 34.015-2002.

Порядок выполнения работы

1. Изучить предлагаемый теоретический материал и стандарт СТ РК 34.015-2002.
2. Подготовить техническое задание на разработку заданной системы.
3. Построить отчёт, включающий разработанное ТЗ.

Контрольные вопросы:

1. Структура технического задания по СТ РК.

2. Какие допущения регламентирует СТ РК при написании ТЗ?

3. В каких разделах ТЗ используется материал предыдущих лабораторных работ?

4. Какими СТ РК и руководящими документами нужно руководствоваться при написании раздела «Требования к документированию»?

5. Какой СТ РК регламентирует оформление ТЗ?

6. В каком разделе указывают полное наименование системы и ее условное обозначение?

7. В разделе «Характеристики объекта автоматизации» приводят: ?

8. Раздел «Требования к системе» состоит из следующих подразделов: ?

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

Рекомендуемая литература

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

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

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

4 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

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

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

Лабораторная работа № 5 (6 часов)

Методология анализа защищенности информационной системы

Цель работы: выявление значимых составляющих информационной безопасности и характеристик информационной системы в конкретных ситуациях, провести анализ нарушений информационной безопасности, научиться работать с нормативными документами в области защиты информации, научиться составлять практические рекомендации по защите информации на основе ГОСТа, научиться выполнять оценку защищенности информационной системы.

Задачи

1. Проанализируйте данные нарушения:

1.1. Сотрудники сидят в интернете на развлекательных сайтах по 4 часа. Играют в игры на работе. Перекладывают свои обязанности на других. Сотрудники копируют конфиденциальные данные компании. Сотрудники одновременно работают на другой работе. Сотрудники работают на конкурента. Сотрудник хочет создать собственную конкурентную компанию. Сотрудники распространяют государственную тайну.

1.2. Используется потенциальное опасное ПО, содержащее уязвимости, позволяющие скрытую передачу данных, дающие возможность деструктивного влияния на ИТ инфраструктуру компании. Выясняется, что административные пароли передаются по открытым каналам. Сотрудники используют средства удаленного управления. Администраторы сделали бреши в межсетевом периметре компании для удобства. Оставлены закладки в самописном программном обеспечении.

1.3. Как предотвратить потерю информации?

1.4. Что следует предпринять для устранения данных нарушений?

2. Определение класса ИС организации (согласно варианту лабораторных работ № 2,3,4) в соответствии с Приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135 «Об утверждении Правил классификации объектов информатизации и классификатор объектов информатизации» https://adilet.zan.kz/rus/docs/V1600013349#z4

2.1. Определите принадлежность объекта информатизации к одной из категорий классификатора объектов информатизации

2.2. Определите схему классификации объектов информатизации в рамках определенной категории вашей организации

2.3. Выберите характеристики категории - совокупность отличительных параметров классификатора объектов информатизации, характеризующих объект информатизации, суммарное значение которых определяет класс объекта информатизации.

2.4. Определите к какому классу относится информационная система вашей организации.

2.5. Заполните таблицы Классификационная оценка ИС, Результаты расчета категорий ИС, Классификационные характеристики ИС.

3. Управление рисками.

3.1. Выполните идентификацию рисков в отношении перечня идентифицированных и классифицированных активов ИС предприятия.

3.2. Выполните выбор критериев принятия идентифицированных рисков.

3.3. Выполните идентификацию уязвимостей и последствий инцидентов ИБ.

3.4. Оцените тяжесть влияния (воздействия) последствий от реализации рисков ИБ, вероятность возникновения (реализации) риска ИБ, вычислите уровень риска.

3.5. Сформируйте каталог угроз (рисков) ИБ, включающего оценку (переоценку) идентифицированных рисков в соответствии с требованиями стандарта Республики Казахстан СТ РК ISO/IEC 27005 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности».

3.6. Сформируйте Карту рисков.

3.7. Разработайте план обработки угроз (рисков) ИБ, содержащий мероприятия по их нейтрализации или снижению, рассчитайте остаточный риск, относительно которого принимается решение о завершении обработки риска.

Порядок выполнения работы

1. Изучить предлагаемый теоретический материал, Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»; Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135 «Об утверждении Правил классификации объектов информатизации и классификатор объектов информатизации», стандарты СТ РК ISO/IEC 27005 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности», СТ РК ИСО/МЭК 31010 «Менеджмент риска. Методы оценки рисков».
2. Заполнить таблицы согласно заданиям, из п. 2 и 3.
3. Сформировать Карту рисков.
4. Разработать план обработки угроз (рисков).
5. Построить отчёт, включающий разработанные таблицы и карту рисков.

Контрольные вопросы:

1. Что принято называть угрозой информационной безопасности?

2. Какие составляющие информационной безопасности должны быть соблюдены?

3. Что будет если одна из составляющих информационной безопасности будет нарушена?

4. Что понимается под термином информационный объект?

5. Что представляет собой угроза права собственности?

6. Какова классификация методов защиты информации, в том числе по характеру проводимых мероприятий?

7. Какова классификация угроз информационной безопасности?

8. Для чего нужны законодательные меры в области информационной безопасности?

9. Какими документами регулируется информационная безопасность в РК?

10. Какие основополагающие документы в области информационной безопасности вам известны?

Рекомендуемая литература

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

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

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

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

Лабораторная работа № 6 (4 часа)

Технология сертификации средств защиты информации

Цель работы: Получение навыков работы с документами по сертификации в области информационной безопасности, изучение основных положений методики испытаний объектов информатизации по требованиям безопасности информации.

Задачи

1 Основные положения методики испытаний по требованиям безопасности информации

2 Контроль состава и содержания документации

3 Ознакомиться с нормативными документами, регламентирующими работу испытательной лаборатории

Порядок выполнения работы

1 Составить актуальный перечень нормативных документов по сертификации в области информационной безопасности на текущий момент.

2 Укажите необходимость и порядок процедуры сертификации средств защиты информации.

3 Составьте перечень объектов информатизации, которые перед вводом в промышленную эксплуатацию в обязательном порядке проходят процедуру испытаний на соответствие требованиям информационной безопасности.

4 Выбрать любое свободное программное обеспечение (ПО). Далее необходимо найти всю возможную информацию о продукте (техническую и функциональную) необходимую для его дальнейшей сертификации.

5 Определить достаточность найденных материалов для проведения сертификации. Описать каких входные данные дополнительно необходимы для проведения сертификационных работ.

6 Составить заявку на сертификацию в уполномоченный орган по сертификации, приложив необходимый пакет документов

Контрольные вопросы

1. К объектам информатизации, подлежащим обязательным испытаниям на соответствие требованиям ИБ, относят?

2. Методика проведения испытаний объектов информатизации включает?

3. Проведение испытаний объектов информатизации на соответствие требованиям информационной безопасности регламентируется?

4. Испытания на соответствие требованиям ИБ включают следующие виды работ?

5. Критериями по включению ПО в реестр доверенного ПО и продукции электронной промышленности являются?

6. Что такое сертификация?

7. Назовите основные руководящие документы, относящиеся к сертификации средств защиты информации.

8. Какие документы необходимы разработчику ПО для успешного прохождения сертификации? Где можно найти требования к документации?

Рекомендуемая литература

1. Закон РК «Об информатизации» от 24 ноября 2015 года № 418-V.

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

3 СТ РК ISO/IEC 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ.

4 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».

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

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

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