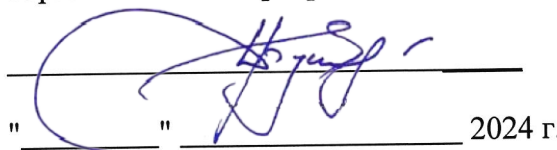


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДАЮ

Руководитель основной профессиональной
образовательной программы


" " 2024 г.

РАБОЧАЯ ПРОГРАММА

Дисциплины

Б1.О.23 Основы управления информационной безопасностью

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

10.03.01 Информационная безопасность

профиль

*Безопасность автоматизированных систем (по отрасли или в сфере
профессиональной деятельности)*

Квалификация

Бакалавр

Форма обучения

очная

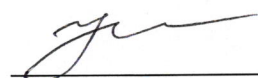
РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск
2024

Рабочая программа дисциплины Основы управления информационной безопасностью составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность.

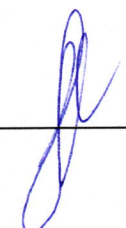
Программу составил(и):

Мазур И.К., доцент кафедры информатики,



Рабочая программа дисциплины Основы управления информационной безопасностью утверждена на заседании кафедры информатики, протокол № 8 от 19.03.2024 г.

Исполняющий обязанности
заведующего кафедрой информатики



Осипов Г.С.

1. Цель и задачи дисциплины

Цель дисциплины

Овладение основными принципами управления уровнями информационной безопасности защищаемых ресурсов организации, формирование системы знаний о принципах, методах, подходах и инструментах эффективного управления информационной безопасностью в современной организации.

Задачи дисциплины

- знакомство обучающихся с основами технологии обеспечения информационной безопасности;
- формирование у обучающихся понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем;
- получение студентами знаний о структуре и принципах построения политики информационной безопасности организации.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы управления информационной безопасностью» относится к разделу обязательных дисциплин подготовки студентов по направлению подготовки бакалавров 10.03.01 Информационная безопасность.

Пререквизиты дисциплины:

Для освоения данной дисциплины студент должен владеть основными понятиями дисциплин Основы информационной безопасности, Организационное и правовое обеспечение информационной безопасности.

Постреквизиты дисциплины:

Знания, умения и навыки, полученные в процессе изучения данного курса, могут быть использованы студентами при изучении дисциплины «Комплексное обеспечение защиты информации объекта информатизации», «Методы и средства криптографической защиты информации», «Защита информации от утечки по техническим каналам», «Программно-аппаратные средства защиты информации». Освоение данной дисциплины должно подготовить студентов к профессиональной деятельности в области информационной безопасности, призваны подготовить к прохождению преддипломной практики, написанию выпускной квалификационной работы.

3. Формируемые компетенции и индикаторы их достижения по дисциплине

| Код компетенции | Содержание компетенции | Код и наименование индикатора достижения компетенции |
|-----------------|---|---|
| УК-3 | Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде | УК-3.1. Знать основные приемы и нормы социального взаимодействия; основные понятия и методы конфликтологии, технологии межличностной и групповой коммуникации в деловом взаимодействии. УК-3.2. Уметь устанавливать и поддерживать контакты, обеспечивающие успешную работу в коллективе; применять основные методы и нормы социального взаимодействия для реализации своей роли и взаимодействия внутри команды. УК-3.3. |

| | | |
|---------|---|--|
| | | Владеть простейшими методами и приемами социального взаимодействия и работы в команде. |
| ОПК-1 | Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства | ОПК-1.1 - Знает сущность и понятие информационной безопасности, характеристику ее составляющих, а также основные средства и способы обеспечения информационной безопасности; ОПК-1.2 - Умеет проводить анализ и выбор средств и способов обеспечения информационной безопасности; ОПК-1.3 - Владеет практическими навыками поиска необходимой информации и обеспечения информационной безопасности при решении задач в области профессиональной деятельности. |
| ОПК-5 | Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности | ОПК-5.1 - Знает основные виды и порядок применения нормативных и методических документов, а также порядок соблюдения законодательных ограничений в сфере профессиональной деятельности; ОПК-5.2 - Умеет использовать основные методы правовой оценки различных подходов решения задач в сфере профессиональной деятельности; ОПК-5.3 - Владеет навыками разработки текстовой документации в области профессиональной деятельности в соответствии с нормативными требованиями, регламентирующими деятельность по защите информации. |
| ОПК-10 | Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты; | ОПК-10.1 - Знает принципы формирования политики информационной безопасности автоматизированных систем; ОПК-10.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; ОПК-10.3 - Владеет навыками разработки политики безопасности информации автоматизированных систем |
| ОПК-4.1 | Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах | ОПК-4.1.1 - Знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; ОПК-4.1.2 - Умеет определять подлежащие защите информационные ресурсы, определять параметры настройки программного обеспечения, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; ОПК-4.1.3 - Владеет навыками разработки политики безопасности информации автоматизированных систем. |

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет **4** зачетные единицы (**144** академических часа).

| Вид работы | Трудоемкость, акад. часов | |
|--|---------------------------|------------|
| | семестр | всего |
| | 7 | |
| Общая трудоемкость | 144 | 144 |
| Контактная работа: | 50 | 50 |
| Лекции (Лек) | 14 | 14 |
| Лабораторные работы (Лаб) | 30 | 30 |
| Контактная работа в период теоретического обучения (КонтТО) (Проведение текущих консультаций и индивидуальная работа со студентами) | 5 | 5 |
| Контактная работа в период промежуточной аттестации (КонтПА) | 1 | 1 |
| Промежуточная аттестация - экзамен | 26 | 26 |
| Самостоятельная работа: | 68 | 68 |
| - самостоятельное изучение разделов (раздел 1); | 0 | 0 |
| - самоподготовка (проработка и повторение лекционного материала, материала учебников и учебных пособий); | 19 | 19 |
| | 24 | 24 |
| - подготовка к лабораторным занятиям; | 8 | 8 |
| - подготовка к коллоквиумам; | 8 | 8 |
| - подготовка к промежуточной аттестации и т.п.) | 9 | 9 |

4.2. Распределение видов работы и их трудоемкости по разделам дисциплины (модуля)

| № п/п | Раздел дисциплины/ темы | | Виды учебной работы (в часах) | | | | Формы текущего контроля успеваемости, промежуточной аттестации |
|----------|--|---------|----------------------------------|-------------------------|-------------------------|---------------------------|--|
| | | | контактная | | | Самостоятельная работа | |
| | | семестр | Лекции | Практические занятия | Лабораторные занятия | | |
| 1. | Анализ объекта защиты | 8 | 2 | | 6 | 14 | Устный опрос по теме лекции. Проверка домашнего задания. |
| 2. | Модель угроз и модель нарушителя | | 4 | | 6 | 14 | Устный опрос по теме лекции. Проверка домашнего задания. |
| 3. | Основы управления рисками информационной безопасности | | 2 | | 6 | 10 | Устный опрос по теме лекции. Проверка домашнего задания. |

| | | | | | | | |
|----|---|--|-----------|--|-----------|-----------|---|
| 4. | Система управления информационной безопасностью | | 2 | | 6 | 10 | Устный опрос по теме лекции. Проверка домашнего задания. |
| 5. | Политика информационной безопасности | | 4 | | 6 | 10 | Устный опрос по теме лекции. Проверка домашнего задания. |
| 6. | экзамен | | 0 | | 0 | 10 | |
| | итого | | 14 | | 30 | 68 | |

4.3. Содержание разделов дисциплины

Тема 1. Анализ объекта защиты

Технология анализа объекта защиты. Типы информационных систем. Методы оценки ущерба от реализации угроз информационной безопасности. Комплекс стандартов в области информационной безопасности.

Тема 2. Модель угроз и модель нарушителя

Подходы к формированию модели нарушителя и модели угроз. Требования регуляторов к формированию модели нарушителя и модели угроз.

Тема 3. Основы управления рисками информационной безопасности

Основные определения и положения по управлению рисками. Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Методики анализа рисков ИБ. Источники информации об активах организации. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Использование результатов анализа рисков ИБ. Основные положения стандартов в области управления рисками информационной безопасности.

Тема 4. Система управления информационной безопасностью

Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Понятие, области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные подразделения организации, кадры). Описание области деятельности (структура и содержание документа). Ролевая структура СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Организация управления персоналом в контексте обеспечения информационной безопасности.

Тема 5. Политика информационной безопасности

Цели Политики СУИБ. Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ. Основные положения стандартов в области регламентации обеспечения информационной безопасности.

4.4. Темы и планы лабораторных занятий

Лабораторное занятие №1 (6 ч.)

Тема Анализ объекта защиты

Вопросы для обсуждения:

1. Стандартизация систем и процессов управления информационной безопасностью
2. Формальное описание структуры информационной системы.
3. Определение типа системы и требований к ней по уровню защиты информации
4. Оценка ущерба от реализации угроз информационной безопасности

Лабораторное занятие №2 (6 ч.)

Тема **Модель угроз и модель нарушителя**

Вопросы для обсуждения:

1. Определение угроз и каналов утечки информации от действий нарушителя.
2. Построение модели угроз для выбранного объекта информатизации.
3. Отбор параметров модели

Лабораторное занятие №3 (6 ч.)

Тема **Основы управления рисками информационной безопасности**

Вопросы для обсуждения:

1. Анализ рисков информационной безопасности на основе построения модели информационных потоков.
2. Разработка методики оценки рисков информационной безопасности
3. Выделение типов информации и формирование требований по защите

Лабораторное занятие №4 (6 ч.)

Тема **Система управления информационной безопасностью**

Вопросы для обсуждения:

1. Формирование требований к системе защиты информации.
2. Концептуальные основы построения защиты информационных процессов от несанкционированного доступа в компьютерных системах
3. Управление персоналом в контексте обеспечения информационной безопасности.

Лабораторное занятие №5 (6 ч.)

Тема **Политика информационной безопасности**

Вопросы для обсуждения:

1. Цели Политики СУИБ. Структура и содержание Политики СУИБ
2. Формирование требований к политике информационной безопасности.
3. Источники информации для разработки Политики СУИБ.

5. Темы дисциплины (модуля) для самостоятельного изучения

Не предусмотрены

6. Образовательные технологии

| № п/п | Наименование раздела | Виды учебных занятий | Образовательные технологии |
|-------|----------------------------------|--------------------------|--|
| 1. | Анализ объекта защиты | Лекция 1 | Традиционная лекция в ауд. с мультимедиа проектором |
| | | Лабораторные занятия 1-3 | Лабораторное занятие в компьютерном классе. |
| | | Самостоятельная работа | Изучение материала по теме лекции, подготовка домашнего задания. |
| 2. | Модель угроз и модель нарушителя | Лекции 2,3 | Традиционная лекция в ауд. с мультимедиа проектором |
| | | Лабораторные занятия 4-6 | Лабораторное занятие в компьютерном классе. |
| | | Самостоятельная работа | Изучение материала по теме лекции, подготовка домашнего задания. |

| | | | |
|----|---|----------------------------|--|
| 3. | Основы управления рисками информационной безопасности | Лекция 4 | Традиционная лекция в ауд. с мультимедиа проектором |
| | | Лабораторные занятия 7-9 | Лабораторное занятие в компьютерном классе. |
| | | Самостоятельная работа | Изучение материала по теме лекции, подготовка домашнего задания. |
| 4. | Система управления информационной безопасностью | Лекция 5 | Традиционная лекция в ауд. с мультимедиа проектором |
| | | Лабораторные занятия 10-12 | Лабораторное занятие в компьютерном классе. |
| | | Самостоятельная работа | Изучение материала по теме лекции, подготовка домашнего задания. |
| 5. | Политика информационной безопасности | Лекции 6,7 | Традиционная лекция в ауд. с мультимедиа проектором |
| | | Лабораторные занятия 13-15 | Лабораторное занятие в компьютерном классе. |
| | | Самостоятельная работа | Изучение материала по теме лекции, подготовка домашнего задания. |

7. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (модулю)

Оценочные средства составляются преподавателем самостоятельно при ежегодном обновлении банка средств. Количество вариантов зависит от числа обучающихся.

Задания для текущего контроля

| № раздела дисциплины | Наименование лабораторных работ |
|----------------------|---|
| 1. | Стандарты информационной безопасности. Моделирование деятельности организации Модель автоматизированной ИС |
| 2. | Состав и особенности информационных потоков организации Оценка информационных потоков организации по уровню конфиденциальности Модель угроз и модель нарушителя |
| 3. | Методика оценки рисков информационной безопасности Оценка вероятности реализации каждого вида угроз и оценка усредненных убытков (рисков). Формирование требований по защите информации |
| 4. | Формирование концепции информационной безопасности Требования к системе защиты информации Организационные меры информационной безопасности автоматизированных систем |
| 5. | Разработка политики информационной безопасности: область действия; Объект защиты; стратегия защиты; организационная структура. |

Примерные темы самостоятельной работы

1. Международные и отечественные стандарты информационной безопасности.
2. Моделирование деятельности организации
3. Моделирование автоматизированной ИС
4. Определение состава информационных потоков организации
5. Оценка информационных потоков организации по уровню конфиденциальности
6. Модель угроз и модель нарушителя
7. Методика оценки рисков информационной безопасности
8. Оценка вероятности реализации каждого вида угроз и оценка усредненных убытков (рисков).
9. Формирование требований по защите информации
10. Формирование концепции информационной безопасности
11. Требования к системе защиты информации
12. Организационные меры информационной безопасности автоматизированных систем
13. Определение области действия в политике информационной безопасности.
14. Определение объекта защиты в политике информационной безопасности.
15. Определение стратегии защиты информации в политике информационной безопасности.
16. Определение организационной структуры в политике информационной безопасности

Примерные темы рефератов:

1. Анализ объекта защиты
2. Технология анализа объекта защиты.
3. Типы информационных систем.
4. Методы оценки ущерба от реализации угроз информационной безопасности.
5. Комплекс стандартов в области информационной безопасности.
6. Модель угроз и модель нарушителя
7. Подходы к формированию модели нарушителя и модели угроз.
8. Требования регуляторов к формированию модели нарушителя и модели угроз.
9. Основы управления рисками информационной безопасности
10. Основные определения и положения рисками.
11. Цель процесса анализа рисков ИБ.
12. Этапы и участники процесса анализа рисков ИБ.
13. Методики анализа рисков ИБ.
14. Источники информации об активах организации.
15. Оценка рисков ИБ.
16. Планирование мер по обработке выявленных рисков ИБ.
17. Использование результатов анализа рисков ИБ.
18. Основные положения стандартов в области управления рисками информационной безопасности.
19. Система управления информационной безопасностью
20. Место системы управления информационной безопасностью в рамках общей системы управления предприятием.
21. Этапы разработки и функционирования системы управления информационной безопасностью.
22. Организация управления персоналом в контексте обеспечения информационной безопасности.

Примерные вопросы к экзамену.

1. Цель и этапы анализа объектов защиты.
2. Перечислите этапы оценки рисков информационной безопасности автоматизированных систем.
3. Идентификация и классификация объектов защиты.
4. Подходы к разграничению доступа в рамках организации. Структура документов, регламентирующих разграничение доступа.
5. Подходы к построению модели нарушителя.

6. Классификация нарушителей (ФСТЭК).
7. Классификация угроз безопасности персональных данных (ФСТЭК).
8. Методика определения актуальных угроз (ФСТЭК).
9. Методика оценки ущерба, нанесённого при реализации угроз информационной безопасности.
10. Предоставление сотруднику доступа к конфиденциальной информации. Основные разделы Инструкции по внесению изменений в списки пользователей.
11. Обязанности сотрудников Службы безопасности при обучении и увольнении сотрудников.
12. Упрощённая модель классификации субъектов.
13. Основные положения регламента контроля использования технических средств обработки и передачи информации.
14. Основные положения инструкции по организации парольной защиты.
15. Классификация объектов при составлении аварийного плана.
16. Требования к различным классам объектов и их резервированию.
17. Основные положения плана обеспечения непрерывной работы и восстановления работоспособности.
18. Приведите примеры источников информации об инцидентах информационной безопасности.
19. Приведите требования к формированию политики информационной безопасности организации и учитываемые в ней категории безопасности.
20. Создание СУИБ на предприятии.
21. Методики и технологии управления рисками.
22. Современные методы и средства анализа и управление рисками информационных систем компаний.

8. Система оценивания планируемых результатов обучения

Критерии оценивания:

Критерием оценивания является выполнение самостоятельных заданий, контрольных и лабораторных работ.

Самостоятельные задания, контрольные и лабораторные работы по результатам выполнения и защиты оцениваются с учетом следующих основных параметров:

- своевременное выполнение работы;
- полнота и правильность ответов на вопросы, заданные в ходе защиты работы.

В случае выполнения данных условий, студент имеет возможность сдавать теоретический зачет по вопросам.

Оценка «отлично» выставляется студенту, глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.

Оценка «хорошо» выставляется студенту, твердо знающему программный материал, грамотно и по существу излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.

Оценка «удовлетворительно» выставляется студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

оценка **«неудовлетворительно»** выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, допускающему в ответе или в решении задач грубые ошибки.

| Форма контроля | За одну работу | | Всего | |
|----------------|----------------|--------------|-------------|--------------|
| | Мин. баллов | Макс. баллов | Мин. баллов | Макс. баллов |

| | | | | |
|---|------|------|-----------|------------|
| Текущий контроль: | | | | |
| Активная работа на занятии | 0,25 | 0,5 | 9 | 18 |
| Выполнение домашнего задания | 0,75 | 0,75 | 27 | 27 |
| Выполнение заданий самостоятельной работы | 1 | 3 | 1 | 3 |
| коллоквиум | 1 | 3 | 3 | 9 |
| Промежуточная аттестация (зачет) | | | 20 | 43 |
| Итого за семестр | | | 60 | 100 |

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература:

1. Голиков, А. М. Основы информационной безопасности : учебное пособие / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2017. — 288 с. — ISBN 978-5-868889-467-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/13957.html>
2. Дождилов, В. Г. Краткий энциклопедический словарь по информационной безопасности / В. Г. Дождилов, М. И. Салтан. — Москва : Энергия, 2015. — 239 с. — ISBN 978-5-98420-043-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/5729.html> (дата обращения: 28.03 2024).
3. Мирошников, А. И. Основы управления информационной безопасностью и защита информации : учебное пособие / А. И. Мирошников, А. С. Сысоев. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2022. — 107 с. — ISBN 978-5-00175-160-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/128718.html>
4. Галатенко, В. А. Основы управления информационной безопасностью : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/97562.html>

9.2.дополнительная литература:

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/497002>.
2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/490019>.
3. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/490277>.
4. Семенов Ю.А. Процедуры, диагностики и безопасность в Интернет [Электронный ресурс] / Ю.А. Семенов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 581 с. — 978-5-94774-708-9. — Режим доступа: <http://www.iprbookshop.ru/62827.html>

9.3.Программное обеспечение

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsoft Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Proffesional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия

61031351),

6. Microsoft Internet Security&Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),
7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
9. Microsoft Windows 10 Pro, 64 bit, Rus, OEM, Операционная система
10. Неисключительное право на использование ПО Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition.
11. Неисключительное право на использование ПО Kaspersky Security для виртуальных и облачных сред, Server, VirtSvr, License, Education Renewal
12. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
13. Visual Studio Professional
14. «Антиплагиат. ВУЗ». Лицензионный договор № 5044 от 14.05. 2022 года (ежегодное продление).
15. Учебно-методический комплекс «Информационная безопасность» на 20 учебных мест;
16. Учебно-методический комплекс «Безопасность телекоммуникационных систем» на 20 учебных мест.

9.4. Профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии» (<https://habr.com/>)
2. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- (<https://github.com/>)
3. База книг и публикаций Электронной библиотеки "Наука и Техника" (<http://www.n-t.ru>)
4. Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии (http://window.edu.ru/catalog/?p_rubr=2.2.75.6)
5. Электронная библиотечная система ZNANIUM.COM (<http://znanium.com/>)
6. Цифровая коллекция электронных версий изданий (учебники, учебные пособия, учебно-методические документы, монографии) по экономическим, естественным, техническим и гуманитарным наукам, сгруппированных по тематическим и целевым признакам.
7. Электронная библиотечная система «BOOK.ru» издательства «КноРус медиа» (<https://www.book.ru/>)
8. Интернет-университет информационных технологий (www.intuit.ru)
9. Онлайн среда разработки приложений (ideone.com)
10. Журнал «КомпьютерПресс» (www.compress.ru)
11. Издательство «Открытые системы» (www.osp.ru)
12. Издание о высоких технологиях (www.cnews.ru)
13. Polpred.com Обзор СМИ (<http://polpred.com/>)
14. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru>)
15. Электронная библиотечная система IPRbooks (<http://www.iprbookshop.ru>)
16. Электронная библиотечная система Национальная электронная библиотека (<https://нэб.рф>)
17. Электронная библиотечная система Юрайт (<http://www.biblio-online.ru>)

10. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

Учебные и учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

Для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

Для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

Для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

Для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

для слепых и слабовидящих:

- автоматизированным рабочим местом для людей с нарушением зрения;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемые эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

11. Материально-техническое обеспечение дисциплины (модуля)

Для преподавания и изучения дисциплины используется лекционная аудитория, обеспеченная мультимедиа проектором и сопутствующим оборудованием, интерактивной доской. Используются УМК дисциплины (на бумажном и электронном носителях), фонд научной библиотеки университета, методические и учебно-методические материалы кафедры информатики.

К рабочей программе прилагаются:

Приложение 1 – Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю);

Приложение 2 – Методические указания для обучающихся по освоению дисциплины (модуля).