Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Амурский государственный университет"

УТВЕРЖДАЮ
Проректор по учебной и научной работе
Лейфа А.В. Лейфа
18 апреля 2024 г.

РАБОЧАЯ ПРОГРАММА
«ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

Направление подготовки 10.03.01 Информационная безопасность

Направленность (профиль) образовательной программы – Безопасность автоматизированных систем (по отраслям или в сфере профессиональной деятельности)

Квалификация выпускника – Бакалавр

Год набора – 2024

Форма обучения – Очная

Курс 4 Семестр 7

Зачет с оценкой 7 сем

Общая трудоемкость дисциплины 144.0 (академ. час), 4.00 (з.е)

Составитель С.Г. Самохвалова, доцент, канд. техн. наук

Институт компьютерных и инженерных наук

Кафедра информационной безопасности

2024

Рабочая программа составлена на основании Федерального государственного образовательного стандарта ВО для направления подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17.11.20 № 1427

Рабочая программа обсуждена на заседании кафедры информационной безопасности

01.02.2024 г. , протокол № 8

Заведующий кафедрой Никифорова Л.В. Никифорова

СОГЛАСОВАНО
Учебно-методическое управление
Чалкина Н.А. Чалкина
18 апреля 2024 г.

СОГЛАСОВАНО
Выпускающая кафедра
Никифорова Л.В. Никифорова
18 апреля 2024 г.

СОГЛАСОВАНО
Научная библиотека
Петрович О.В. Петрович
18 апреля 2024 г.

СОГЛАСОВАНО
Центр цифровой трансформации и технического обеспечения
Тодосейчук А.А. Тодосейчук
18 апреля 2024 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины:

Овладение основными принципами управления уровнем информационной безопасности защищаемых ресурсов организации, сформировать систему знаний о принципах, методах, подходах и инструментах эффективного управления информационной безопасностью в современной организации

Задачи дисциплины:

Привитие обучаемым основ культуры обеспечения информационной безопасности; формирование у обучаемых 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 УЧЕБНОГО ПРЕДМЕТА В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Основы управления информационной безопасности» входит в базовую часть дисциплин образовательной программы.

Дисциплина базируется на материале, излагаемом в курсе «Основы информационной безопасностью».

Знания, умения и навыки, полученные в процессе изучения данного курса, могут быть использованы студентами при изучении дисциплин «Организационное и правовое обеспечение информационной безопасности», а также при выполнении выпускной квалификационной работы.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ УЧЕБНОГО ПРЕДМЕТА И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

3.1. Универсальные компетенции и индикаторы их достижения

Категория (группа) универсальных компетенций	Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
Командная работа и лидерство	УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	ИД-1УК-3- знает различные приемы и способы социализации личности и социального взаимодействия ИД-2УК-3-умеет строить отношения с окружаю- щими людьми, с коллегами ИД-3УК-3- имеет практический опыт участия в командной работе, в социальных проектах, распределения ролей в условиях командного взаимодействия

3.2 Общепрофессиональные компетенции и индикаторы их достижения

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
ОПК-5. Способен при- менять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите	ИД-1ОПК-5 знает: основы законодательства Российской Федерации, систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации,

информации в сфере профессиональной деятельности;	правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации, правовые основы организации делопроизводства, виды и состав документации современной организации; ИД-2 ОПК-5 умеет: формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, определять виды документов, необходимых для оформления управленческих действий в профессиональной деятельности, грамотно составлять и оформлять служебные документы. ИД-3 ОПК-5 владеет: действиями (навыками) по применению нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
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;	ИД-1ОПК-10- знать: цели и задачи управления информа- ционной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью, принципы формирования политики информационной безопасности объекта информатизации, принципы организации информационных систем в соответствии с требованиями по защите информации, особенности комплексного подхода к обеспечению информационной безопасности организации ИД-2ОПК-10- уметь: разрабатывать модели угроз и модели нарушителя объекта информатизации, оценивать информационные риски объекта информатизации, определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ИД-3ОПК-10- иметь навыки: участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению

	информационной безопасности, управлять процессом их реализации на объекте защиты;

4. СТРУКТУРА УЧЕБНОГО ПРЕДМЕТА

Общая трудоемкость учебного предмета составляет 4.00 зачетных единицы, 144.0 академических часов.

1 – № п/п

2 – Тема (раздел) учебного предмета, курсовая работа (проект), промежуточная аттестация

3 – Семестр

4 – Виды контактной работы и трудоемкость (в академических часах)

4.1 – Л (Лекции)

4.2 – Лекции в виде практической подготовки

4.3 – ПЗ (Практические занятия)

4.4 – Практические занятия в виде практической подготовки

4.5 – ЛР (Лабораторные работы)

4.6 – Лабораторные работы в виде практической подготовки

4.7 – ИКР (Иная контактная работа)

4.8 – КТО (Контроль теоретического обучения)

4.9 – КЭ (Контроль на экзамене)

5 – Контроль (в академических часах)

6 – Самостоятельная работа (в академических часах)

7 – Формы текущего контроля успеваемости

1	2	3	4									5	6	7
			4.1	4.2	4.3	4.4	4.5	4.6	4.7	4.8	4.9			
1	Анализ объекта защиты	7	2		4								14	опрос
2	Модель угроз и модель нарушителя	7	4		4		4						20	опрос
3	Основы управления рисками ИБ.	7	4		2		4						17	опрос
4	Система управления информационной безопасностью	7	4		2		4						17	опрос
5	Политика информационной безопасности	7	4		6		6						21.8	опрос
6	Зачет с оценкой	7								0.2				
	Итого		18.0		18.0		18.0		0.0	0.2	0.0	0.0	89.8	

5. СОДЕРЖАНИЕ УЧЕБНОГО ПРЕДМЕТА

5.1. Лекции

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
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.
2	Модель угроз и модель нарушителя	Подходы к формированию модели нарушителя и модели угроз. Требования регуляторов к формированию модели нарушителя и модели угроз
3	Основы управления рисками ИБ.	Основные определения и положения 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.
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.
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.

5.2. Практические занятия

Наименование темы	Содержание темы
Анализ объекта защиты	Формальное описание структуры информационной системы.
Модель угроз и модель нарушителя	Составление модели угроз информационной системе.
Основы управления рисками ИБ.	Анализ рисков информационной безопасности на основе построения модели информационных потоков. Разработка методики оценки рисков ИБ
Система управления	Формирование требований к системе защиты

информационной безопасностью	информации
Политика информационной безопасности	Формирование требований к политике информационной безопасности.
Политика информационной безопасности	Разработка Политики

5.3. Лабораторные занятия

Наименование темы	Содержание темы
Модель угроз и модель нарушителя	Построение модели угроз для выбранного объекта информатизации
Основы управления рисками ИБ	Выделение типов информации и формирование требований по защите
Система управления информационной безопасностью	Концептуальные основы построения защиты информационных процессов от несанкционированного доступа в компьютерных системах
Политика информационной безопасности	Источники информации для разработки Политики СУИБ.

6. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)	Трудоемкость в академических часах
1	Анализ объекта защиты	Работа с лекционным материалом. Подготовка к опросу. Подготовка к практическим и лабораторным занятиям.	14
2	Модель угроз и модель нарушителя	Работа с лекционным материалом. Подготовка к опросу. Подготовка к практическим и лабораторным занятиям.	20
3	Основы управления рисками ИБ.	Работа с лекционным материалом. Подготовка к опросу. Подготовка к практическим и лабораторным занятиям.	17
4	Система управления информационной безопасностью	Работа с лекционным материалом. Подготовка к опросу. Подготовка к практическим и лабораторным занятиям.	17
5	Политика информационной безопасности	Работа с лекционным материалом. Подготовка к опросу. Подготовка к практическим и лабораторным занятиям.	21.8

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе подготовки по дисциплине используется совокупность методов и средств обучения, позволяющих осуществлять целенаправленное методическое руководство учебно-познавательной деятельностью бакалавров, в том числе на основе интеграции информационных и традиционных педагогических технологий.

На занятиях используются методы активного обучения: лекция с заранее запланированными ошибками (лекция- провокация), лекция с разбором конкретных ситуаций, мозговой штурм. Рекомендуется использование информационных технологий при организации коммуникации со студентами для представления информации, выдачи рекомендаций и консультирования по оперативным вопросам (электронная почта), использование мультимедиа- средств при проведении лекционных, практических и лабораторных занятий.

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Промежуточная аттестация по итогам освоения дисциплины: зачет с оценкой
Вопросы к зачету с оценкой

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.

9. УЧЕБНО- МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРЕДМЕТА

а) литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/ bcode/544290 (дата обращения: 22.03.2024).
2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная

платформа Юрайт [сайт]. — URL: https:// urait.ru/ bcode/537000 (дата обращения: 22.03.2024).
3. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/ bcode/537247 (дата обращения: 22.03.2024).
4. Дождиков, В. Г. Краткий энциклопедический словарь по информационной безопасности / В. Г. Дождиков, М. И. Салтан. — Москва : Издательский дом ЭНЕРГИЯ, 2012. — 240 с. — ISBN 978-5-98908-050-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https:// www.iprbookshop.ru/121962.html (дата обращения: 22.03.2024). — Режим доступа: для авторизир. пользователей
5. Голиков, А. М. Основы информационной безопасности : учебное пособие / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2007. — 288 с. — ISBN 978-5-868889-467-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https:// www.iprbookshop.ru/13957.html (дата обращения: 22.03.2024). — Режим доступа: для авторизир. пользователей

б) программное обеспечение и Интернет-ресурсы

№	Наименование	Описание
1	Google Chrome	Бесплатное распространение по лицензии google chromium http:// code.google.com/ intl/ ru/ chromium/ terms.html на условиях https:// www.google.com/ chrome/ browser/privacy/eula_text.html.
2	Операционная система Linux	GNU-лицензия (GNU General Public License)
3	LibreOffice	Бесплатное распространение по лицензии GNU LGPL https://ru.libreoffice.org/about-us/license/
4	Система защиты информации от несанкционированного доступа Dallas Lock	Договор о сотрудничестве с образовательным учреждением 127-17-153/1.
5	http://www.intuit.ru/	Интернет университет информационных технологи, содержит бесплатные учебные курсы, учебники и методические пособия по всем направлениям подготовки
6	https://urait.ru	Электронная библиотечная система «Юрайт». Фонд электронной библиотеки составляет более 4000 наименований и постоянно пополняется новинками, в большинстве своем это учебники и учебные пособия для всех уровней профессионального образования от ведущих научных школ с соблюдением требований новых ФГОСов
7	http:// www.iprbookshop.ru	Электронно- библиотечная система IPRbooks — научно- образовательный ресурс для решения задач обучения в России и за рубежом. ЭБС IPRbooks в полном объеме соответствует требованиям законодательства РФ в сфере образования

в) профессиональные базы данных и информационные справочные системы

№	Наименование	Описание
1	http:// www.ict.edu.ru/ about	Портал "Информационно- коммуникационные технологии в образовании" входит в систему федеральных образовательных порталов и нацелен на обеспечение комплексной информационной поддержки образования в области современных информационных и телекоммуникационных технологий, а также деятельности по применению ИКТ в сфере образования.
2	www.elibrary.ru	Крупнейший российский информационный портал в области науки, технологии, медицины и образования
3	www.iop.org	В свободном доступе представлены все оглавления и все рефераты. Полные тексты всех статей во всех журналах находятся в свободном доступе в течение 30 дней после даты их онлайновой публикации.

10. МАТЕРИАЛЬНО- ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРЕДМЕТА

Занятия по дисциплине проводятся в специальных помещениях, представляющих собой учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Все помещения, в которых проводятся занятия, соответствуют действующим противопожарным правилам и нормам.

Каждый обучающийся обеспечен индивидуальным неограниченным доступом к электронно- библиотечным системам и к электронной информационно- образовательной среде университета.

Самостоятельная работа обучающихся осуществляется в помещениях, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно- образовательную среду университета.