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
« 1 » сентября 2023 г.

РАБОЧАЯ ПРОГРАММА
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки 09.03.04 Программная инженерия

Направленность (профиль) образовательной программы – Программная инженерия

Квалификация выпускника – Бакалавр

Год набора – 2023

Форма обучения – Очная

Курс 4 Семестр 7

Экзамен 7 сем

Общая трудоемкость дисциплины 180.0 (академ. час), 5.00 (з.е)

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

Факультет математики и информатики

Кафедра информационной безопасности

2023

Рабочая программа составлена на основании Федерального государственного образовательного стандарта ВО для направления подготовки 09.03.04 Программная инженерия, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 19.09.17 № 920

Рабочая программа обсуждена на заседании кафедры информационной безопасности

01.09.2023 г. , протокол № 1

Заведующий кафедрой Никифорова Л.В. Никифорова

СОГЛАСОВАНО
Учебно-методическое управление
Чалкина Н.А. Чалкина
« 1 » сентября 2023 г.

СОГЛАСОВАНО
Выпускающая кафедра
Бушманов А.В. Бушманов
« 1 » сентября 2023 г.

СОГЛАСОВАНО
Научная библиотека
Петрович О.В. Петрович
« 1 » сентября 2023 г.

СОГЛАСОВАНО
Центр цифровой трансформации и технического обеспечения
Тодосейчук А.А. Тодосейчук
« 1 » сентября 2023 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины:

Заложить терминологический фундамент, рассмотреть основные общеметодологические принципы теории информационной безопасности; изучить методы и средства обеспечения ИБ, методы нарушения конфиденциальности, целостности и доступности информации и противодействия этим нарушениям

Задачи дисциплины:

Формирование знаний у студентов о современном состоянии проблемы обеспечения информационной безопасности при использовании компьютерных технологий, существующих угрозах, видах обеспечения информационной безопасности, методах и средствах защиты информации и основах построения комплексных систем защиты.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность» относится к базовой части дисциплин образовательной программы. Данный курс базируется на знаниях, полученных в области информатики, операционных систем, сети и телекоммуникации, базы данных. Знания, умения и навыки, полученные в процессе изучения данного курса, могут быть использованы студентами для подготовки выпускной квалификационной работы.

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

3.1 Общепрофессиональные компетенции и индикаторы их достижения

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИД-1ОПК-3- знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ИД-2ОПК-3- уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности ИД-3ОПК-3- иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

4. СТРУКТУРА ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5.00 зачетных единицы, 180.0 академических часов.

1 – № п/п

2 – Тема (раздел) дисциплины, 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	Основные понятия и определения в области информационной безопасности	7	2										4	опрос
2	Угрозы информационной безопасности. Каналы утечки информации	7	2		2		6						12	тест
3	Вредоносное ПО. Компьютерные вирусы и средства защиты от них.	7	2				6						10	тест
4	Правовое обеспечение информационной безопасности	7	2		2								6	тест
5	Стандарты информационной безопасности	7	2										8	тест
6	Административный уровень информационной безопасности	7	2		4								10	тест

7	Процедурный уровень информационной безопасности	7	2										10	тест
8	Программно-технические методы защиты информационной безопасности	7	4		8		22						16	тест
9	Экзамен	7									0.3	35.7		
	Итого		18.0		16.0		34.0		0.0	0.0	0.3	35.7	76.0	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Лекции

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
1	Основные понятия и определения в области информационной безопасности	Основные понятия и определения, относящиеся к ИБ. Необходимость защиты информации. Основные задачи обеспечения защиты информации. Объекты, цели и задачи защиты информации
2	Угрозы информационной безопасности. Каналы утечки информации	Понятие угрозы. Классификация видов угроз ИБ по различным признакам. Угрозы доступности, целостности и конфиденциальности. Классификация атак. Сетевые атаки. Окно опасности.
3	Вредоносное ПО. Компьютерные вирусы и средства защиты от них.	Понятие компьютерного вируса. Признаки появления вируса. Классификация вирусов. Вирусная сигнатура. Антивирусные программы. Программы «сторожа», ревизоры, доктора, детекторы, вакцины
4	Правовое обеспечение информационной безопасности	Основные функции правовой базы. Законодательство РФ в области защиты информации. Понятие государственная тайна, коммерческая тайна. Профессиональная тайна, служебная тайна. Организация работы с персональными данными.
5	Стандарты информационной безопасности	Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США ("Оранжевая книга"). Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности. Руководящие документы ФСТЭК России. Рекомендации X.800.
6	Административный уровень информационной безопасности	Административный уровень информационной безопасности: основные понятия. Политика безопасности. Программа безопасности. Концепция информационной безопасности
7	Процедурный уровень информационной	Организация внутриобъектового и пропускного режимов на предприятиях. Управление

	безопасности	персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ. Организация подготовки и проведения заседаний по конфиденциальным вопросам. Защита информации при публикаторской деятельности, при рекламной деятельности. Защита информации при работе с посетителями. Организация работы с документами
8	Программно- технические методы защиты информационной безопасности	Основные понятия программно- технического уровня ИБ. Архитектурная безопасность. Парольная аутентификация. Одноразовые пароли. Идентификация/ аутентификация с помощью биометрических данных. Протоколирование. Активный аудит. Функциональные компоненты и архитектура. Криптография. Стеганография. Управление доступом.

5.2. Практические занятия

Наименование темы	Содержание темы
Угрозы информационной безопасности. Каналы утечки информации	Построение модели угроз и модели нарушителя
Правовое обеспечение информационной безопасности	Разработка "Положения об обработке персональных данных".
Административный уровень информационной безопасности	Разработка частной политики безопасности.
Программно- технические методы защиты информационной безопасности	Шифры перестановок. Шифры замены
Программно- технические методы защиты информационной безопасности	Количественная оценка стойкости парольной защиты

5.3. Лабораторные занятия

Наименование темы	Содержание темы
Угрозы информационной безопасности. Каналы утечки информации	Защита информации в пакетах офисных программ.
Угрозы информационной безопасности. Каналы утечки информации	Резервное копирование.
Вредоносное ПО. Компьютерные вирусы и средства защиты от них.	Использование антивирусных программ.
Вредоносное ПО. Компьютерные вирусы и средства защиты от них.	Восстановление удалённой информации. Безвозвратное удаление.
Программно- технические	Система защиты информации «Страж NT»

методы защиты информационной безопасности	
Программно- технические методы защиты информационной безопасности	Система защиты информации от несанкционированного доступа Dallas Lock
Программно- технические методы защиты информационной безопасности	Разграничение прав доступа.
Программно- технические методы защиты информационной безопасности	Контроль целостности
Программно- технические методы защиты информационной безопасности	Восстановление паролей к зашифрованным файлам

6. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)	Трудоемкость в академических часах
1	Основные понятия и определения в области информационной безопасности	Работа с лекционным материалом. Подготовка к тесту	4
2	Угрозы информационной безопасности. Каналы утечки информации	Работа с лекционным материалом. Подготовка к практическим и лабораторным занятиям. Подготовка к тесту	12
3	Вредоносное ПО. Компьютерные вирусы и средства защиты от них.	Работа с лекционным материалом. Подготовка к лабораторным занятиям. Подготовка к тесту	10
4	Правовое обеспечение информационной безопасности	Работа с лекционным материалом Подготовка к практическим занятиям. Подготовка к тесту	6
5	Стандарты информационной безопасности	Работа с лекционным материалом. Подготовка к тесту	8
6	Административный уровень информационной безопасности	Работа с лекционным материалом Подготовка к практическим занятиям Подготовка к тесту	10
7	Процедурный уровень информационной безопасности	Работа с лекционным материалом. Подготовка к тесту	10
8	Программно-	Работа с лекционным материалом	16

	технические методы защиты информационной безопасности	Подготовка к практическим и лабораторным занятиям Подготовка к тесту	

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: экзамен

Вопросы к экзамену

1. Понятие ИБ. Основные составляющие ИБ и их роль при создании ИС.
2. Значение и роль ИБ в современном мире.
3. Реагирование на нарушение режима безопасности, процедуры плановых восстановительных работ.
4. Угрозы ИБ (основные определения) и критерии классификации угроз.
5. Примеры угроз и рисков по всем основным составляющим (аспектам) ИБ.
6. Анализ угроз и рисков ИС с точки зрения ИБ (матрица рисков).
7. Уровни ИБ. Основные задачи и положения, решаемые на каждом уровне.
8. Российское и международное законодательство в области защиты информации.
9. Стандарты и спецификации в области защиты информации, их основные положения и принципы построения.
10. Основные механизмы и сервисы безопасности.
11. Сетевая безопасность, наиболее характерные угрозы для сетевых ИС.
12. Административный уровень ИБ (основные понятия, политика безопасности).
13. Программа безопасности, синхронизация программы безопасности с жизненным циклом систем.
14. Процедурный уровень ИБ, классификация мер этого уровня.
15. Принципы физической и архитектурной безопасности ИС.
16. Идентификация и аутентификация, управление доступом.
17. Управление доступом, технологии, принципы организации, типичные решения.
18. Протоколирование и аудит. Активный и пассивный аудит.
19. Основные методы шифрования, сервисы безопасности, использующие криптографию.
20. Цели, основные этапы и принципы действий злоумышленников, классификация типов злоумышленников.

9. УЧЕБНО- МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) литература

1. Фомин, Д. В. Информационная безопасность [Электронный ресурс]: учеб.- метод. пособие / Д.В. Фомин; АмГУ, ФМиИ. – Благовещенск: Изд-во Амур. гос. ун-та, 2017. - 60 с. http://irbis.amursu.ru/DigitalLibrary/AmurSU_Edition/7371.pdf

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная

платформа Юрайт [сайт]. — URL: https:// urait.ru/ bcode/512268 (дата обращения: 02.02.2023).

3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998 (дата обращения: 02.02.2023).

4. Казарин, О. В. Программно- аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/ bcode/513300 (дата обращения: 02.02.2023).

5. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2023. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/ bcode/519079 (дата обращения: 02.02.2023).

б) программное обеспечение и Интернет-ресурсы

№	Наименование	Описание
1	Ревизор 1 XP	Сублицензионный договор №34/02/ ИБиИТ/697 от 09.08.2013.
2	Страж-NT	Сублицензионный договор №34/02/ ИБиИТ/697 от 09.08.2013.
3	Система защиты информации от несанкционированного доступа Dallas Lock	Договор о сотрудничестве с образовательным учреждением 127-17-153/1.
4	LibreOffice	Бесплатное распространение по лицензии GNU LGPL https://ru.libreoffice.org/about-us/license/
5	Операционная система Linux	GNU-лицензия (GNU General Public License)
6	Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01	Лицензионный договор № РБТ-14/1607-01- ВУЗ на предоставление права использования программы для ЭВМ.
7	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.
8	http:// www.e.lanbook.com	Электронная библиотечная система «Издательства Лань», тематические пакеты: математика, физика, инженерно-технические науки, химия
9	http://www.intuit.ru/	Интернет университет информационных технологи, содержит бесплатные учебные курсы, учебники и методические пособия по всем направлениям подготовки
10	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 ФГОС.

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	https://reestr.minsvyaz.ru	Единый реестр российских программ для электронных вычислительных машин и баз данных. Реестр создан в соответствии со статьей 12.1 Федерального закона «Об информации, информационных технологиях и о защите информации» в целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из РФ, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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