

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

23 мая 2024 г.

РАБОЧАЯ ПРОГРАММА
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки 09.03.01 Информатика и вычислительная техника

Направленность (профиль) образовательной программы – Информатика и вычислительная техника

Квалификация выпускника – Бакалавр

Год набора – 2024

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

Институт компьютерных и инженерных наук

Кафедра информационной безопасности

Рабочая программа составлена на основании Федерального государственного образовательного стандарта ВО для направления подготовки 09.03.01 Информатика и вычислительная техника, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 19.09.17 № 929

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

23 мая 2024 г.

СОГЛАСОВАНО

Выпускающая кафедра

Бушманов А.В. Бушманов

23 мая 2024 г.

СОГЛАСОВАНО

Научная библиотека

Петрович О.В. Петрович

23 мая 2024 г.

СОГЛАСОВАНО

Центр цифровой трансформации и
технического обеспечения

Тодосейчук А.А. Тодосейчук

23 мая 2024 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 УЧЕБНОГО ПРЕДМЕТА 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 УЧЕБНОГО ПРЕДМЕТА И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

3.1 Обще профессиональные компетенции и индикаторы их достижения

| Код и наименование обще профессиональной компетенции | Код и наименование индикатора достижения обще профессиональной 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-1 ОПК-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-2 ОПК-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-3 ОПК-3 Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности |

3.2 Профессиональные компетенции и индикаторы их достижения

| Код и наименование профессиональной компетенции | Код и наименование индикатора достижения профессиональной компетенции |
|---|---|
|---|---|

| | |
|--|---|
| ПК-12 Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения. Способен проводить регламентные работы на сетевых устройствах и программном обеспечении инфокоммуникационной системы | ИД-1 ПК-12 Знать: архитектуру, устройство и функционирование вычислительных систем, коммуникационное оборудование, сетевые протоколы, методы обеспечения информационной безопасности; ИД-2 ПК-12 Уметь: подготавливать протоколы мероприятий; ИД-3 ПК-12 Владеть: практическими навыками администрирования инфокоммуникационной системы, проведение регламентных работ на сетевых устройствах и программном обеспечении |
|--|---|

4. СТРУКТУРА УЧЕБНОГО ПРЕДМЕТА

Общая трудоемкость учебного предмета составляет 5.00 зачетных единицы, 180.0 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 | Основные понятия и определения в области информационной безопасности | 7 | 2 | | | | | | | | | | 4 | опрос |
| 2 | Угрозы информационной безопасности. Каналы утечки информации | 7 | 2 | | 4 | | 6 | | | | | | 12 | тест |
| 3 | Вредоносное | 7 | 2 | | | | 4 | | | | | | 10 | тест |

| | | | | | | | | | | | | | |
|---|--|---|---|------|------|------|-----|-----|-----|------|------|----|-------|
| | ПО. Компьютерные вирусы и средства защиты от них. | | | | | | | | | | | | |
| 4 | Правовое обеспечение информационной безопасности | 7 | 2 | | | | | | | | | 6 | тест |
| 5 | Стандарты информационной безопасности | 7 | 2 | | | | | | | | | 8 | опрос |
| 6 | Административный уровень информационной безопасности | 7 | 2 | | 4 | | | | | | | 10 | тест |
| 7 | Процедурный уровень информационной безопасности | 7 | 2 | | | | 6 | | | | | 10 | тест |
| 8 | Программно-технические методы защиты информационной безопасности | 7 | 4 | | 8 | | 18 | | | | | 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 УЧЕБНОГО ПРЕДМЕТА

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 | Основные функции правовой базы. Законодательство РФ в области защиты |

| | | |
|---|--|--|
| | безопасности | информации. Владельцы защищаемой информации. Понятие государственная тайна, коммерческая тайна. Профессиональная тайна, служебная тайна. |
| 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 безопасности | Организация внутриобъектового и пропускного режимов на предприятиях. Управление 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. |
| Административный уровень информационной безопасности | Разработка "Положения об обработке персональных данных". |
| Административный уровень информационной безопасности | Разработка частной политики безопасности |
| Программно-технические методы защиты информационной безопасности | Изучение традиционных симметричных криптосистем. 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. |
| Процедурный уровень информационной безопасности | Разграничение прав доступа |
| Процедурный уровень информационной безопасности | Журналы ОС Windows |
| Программно-технические методы защиты информационной безопасности | Электронная подпись |
| Программно-технические методы защиты информационной безопасности | Средство шифрования информации Vera Crypt |
| 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 | Работа с лекционным материалом. Подготовка к практическим и лабораторным занятиям. Подготовка к | 10 |

| | | | |
|---|--|---|----|
| | защиты от них. | тесту | |
| 4 | Правовое обеспечение информационной безопасности | Работа с лекционным материалом. Подготовка к практическим и лабораторным занятиям. Подготовка к тесту | 6 |
| 5 | Стандарты информационной безопасности | Работа с лекционным материалом. Подготовка к практическим и лабораторным занятиям. Подготовка к тесту | 8 |
| 6 | Административный уровень информационной безопасности | Работа с лекционным материалом. Подготовка к практическим и лабораторным занятиям. Подготовка к тесту | 10 |
| 7 | Процедурный уровень информационной безопасности | Работа с лекционным материалом. Подготовка к практическим и лабораторным занятиям. Подготовка к тесту | 10 |
| 8 | Программно-технические методы защиты информационной безопасности | Работа с лекционным материалом. Подготовка к практическим и лабораторным занятиям. Подготовка к тесту | 16 |

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 УЧЕБНОГО ПРЕДМЕТА

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. Орлова, И. В. Информатика. Практические задания / И. В. Орлова. — 2-е изд., стер. — Санкт-Петербург : Лань, 2024. — 140 с. — ISBN 978-5-507-47294-9. — Текст : электронный // Лань : электронно- библиотечная система. — URL: <https://e.lanbook.com/book/358664> (дата обращения: 28.03.2024). — Режим доступа: для авториз. пользователей.
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: 28.03.2024).
4. 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: 28.03.2024).
5. 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, 2024. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/538066> (дата обращения: 28.03.2024).
6. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2024. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/543351> (дата обращения: 28.03.2024).

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 | LibreOffice | Бесплатное распространение по лицензии GNU LGPL https://ru.libreoffice.org/about-us/license/ |
| 3 | Операционная система Linux | GNU-лицензия (GNU General Public License) |

| | | |
|---|---|--|
| 4 | Ревизор сети 2.0 | Сублицензионный договор №34/02/ ИБиИТ/697 от 09.08.2013. |
| 5 | Система защиты информации от несанкционированного доступа Dallas Lock | Договор о сотрудничестве с образовательным учреждением 127-17-153/1. |
| 6 | Страж-NT | Сублицензионный договор №34/02/ ИБиИТ/697 от 09.08.2013. |
| 7 | http://www.e.lanbook.com | Электронная библиотечная система «Издательства Лань», тематические пакеты: математика, физика, инженерно-технические науки, химия |
| 8 | 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. |
| 9 | http://www.intuit.ru/ | Интернет университет информационных технологи, содержит бесплатные учебные курсы, учебники и методические пособия по всем направлениям подготовки |

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 | 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 |
| 3 | http://www.informika.ru | Сайт ФГАУ ГНИИ ИТТ «Информика». Институт является государственным научным предприятием, созданным для обеспечения всестороннего развития и продвижения новых информационных технологий в сферах образования и науки России. |
| 4 | www.elibrary.ru | Крупнейший российский информационный портал в области науки, технологии, медицины и образования. |

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.