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
24 мая 2024 г.

РАБОЧАЯ ПРОГРАММА
«ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ»

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 7,8

Экзамен 8 сем

Зачет 7 сем

Общая трудоемкость дисциплины 252.0 (академ. час), 7.00 (з.е)

Составитель Л.В. Никифорова, 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
24 мая 2024 г.

СОГЛАСОВАНО
Выпускающая кафедра
Никифорова Л.В. Никифорова
24 мая 2024 г.

СОГЛАСОВАНО
Научная библиотека
Петрович О.В. Петрович
24 мая 2024 г.

СОГЛАСОВАНО
Центр цифровой трансформации и технического обеспечения
Тодосейчук А.А. Тодосейчук
24 мая 2024 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины:

Практическое закрепление знаний и навыков проектной, научно-исследовательской и организационной деятельности по основным направлениям информационной безопасности, овладение студентами практическими навыками, методами и средствами по обеспечению информационной безопасности в организациях и на предприятиях различных направлений и различных форм собственности.

Задачи дисциплины:

В результате освоения дисциплины студент должен:

- знать руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
- знать содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации;
- применять основные меры по защите информации в автоматизированных системах;
- знать содержание эксплуатационной документации автоматизированной системы.
- знать типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
- знать критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем;
- знать содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем.
- уметь определять подлежащие защите информационные ресурсы автоматизированных систем;
- разрабатывать политики безопасности информации автоматизированных систем;
- определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы;
- осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации;
- устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации;
- проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств;
- создавать, удалять и изменять учетные записи пользователей автоматизированной системы;
- устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации;
- регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах;
- применять типовые программные средства резервирования и восстановления информации в автоматизированных системах;
- документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы.
- уметь осуществлять автономную наладку технических и программных средств системы защиты информации автоматизированной системы;
- уметь устанавливать обновления программного обеспечения автоматизированной системы;
- уметь обнаруживать и устранять неисправности в работе системы защиты информации автоматизированной системы.

2. МЕСТО УЧЕБНОГО ПРЕДМЕТА В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина "Обеспечение безопасности информации в автоматизированных

системах" относится к блоку дисциплин, формируемой участниками образовательных отношений.
Для успешного освоения данной дисциплины необходимы знания, полученные при изучении дисциплины «Языки программирования», «Математический анализ», «Теория информации», «Теория вероятности и математическая статистика», «Основы информационной безопасности». После изучения дисциплины знания, будут использованы при изучении таких дисциплин, как, «Программно-аппаратные средства защиты информации», «Основы управления информационной безопасностью», «Проектирование защищенных автоматизированных систем», при прохождении производственных практик, при написании выпускной квалификационной работы.

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

3.1 Профессиональные компетенции и индикаторы их достижения

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
ПК-2 Способен принимать участие в организации и проведения аудита защищенности информации в автоматизированных системах	ИД-1ПК-2- знать: методы контроля эффективности защиты информации от утечки по техническим каналам ИД-2ПК-2- уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем ИД-3ПК-2 - иметь навык применения инструментальных средств контроля защищенности информации в автоматизированных системах
ПК-5 Способен управлять защитой информации в автоматизированных системах	ИД-1ПК-5- знать: методы защиты информации от утечки по техническим каналам, национальные, межгосударственные и международные стандарты в области защиты информации, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах ИД-2ПК-5- уметь: Оценивать информационные риски в автоматизированных системах, классифицировать и оценивать угрозы безопасности информации ИД-3ПК-5 - иметь навык анализа воздействия изменений конфигурации автоматизированной системы на ее защищенность, анализ изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации
ПК-6 Способен внедрять организационные меры по защите информации в автоматизированных системах	ИД-1ПК-6- знать: организационные меры по защите информации ИД-2ПК-6- уметь: реализовывать правила разграничения доступа персонала к объектам доступа, анализировать программные и программно- аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей

	безопасности информации в автоматизированных системах ИД-3ПК-6 - иметь навык: подготовки документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации

4. СТРУКТУРА УЧЕБНОГО ПРЕДМЕТА

Общая трудоемкость учебного предмета составляет 7.00 зачетных единицы, 252.0 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	Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети	7	4		4		4						5.8	Опрос. Подготовка к практической работе. Выполнение и защита лабораторной работы
2	Основные механизмы защиты	7	4		4		4						6	Опрос. Подготовка к практической работе. Выполнение и защита лабораторной работы

3	Мониторинг и оперативное управление	7	12		12		4						6	Опрос. Подготовка к практической работе. Выполнение и защита лабораторной работы
4	Централизованная инвентаризация ресурсов локальной сети	7	14		14		4						6	Опрос. Подготовка к практической работе. Выполнение и защита лабораторной работы
5	Зачет	7								0.2				Тестирование
6	Инспекции в автоматизированных системах	8	4				10						6	Опрос. Подготовка к лабораторной работе. Выполнение и защита лабораторной работы
7	Централизованная защита от вирусов в локальной сети	8	6				10						6	Опрос. Подготовка к лабораторной работе. Выполнение и защита лабораторной работы
8	Управление системой безопасности автоматизированной системы	8	6										6	Опрос.
9	Централизованный учет и управление программно-аппаратными средствами защиты информации	8	6										6	Опрос.
10	Управление жизненным циклом и аудит средств аутентификации	8	6				14						6	Опрос. Подготовка к лабораторной работе. Выполнение и защита лабораторной

														работы
11	Нормативные требования по управлению средствами защиты информации	8	6										8	Опрос.
12	Экзамен	8							2		0.3	35.7		
	Итого		68.0		34.0		50.0		2.0	0.2	0.3	35.7	61.8	

5. СОДЕРЖАНИЕ УЧЕБНОГО ПРЕДМЕТА

5.1. Лекции

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
1	Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети	Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети; принципы построения комплексных систем защиты информации (КСЗИ).
2	Основные механизмы защиты	Основные механизмы защиты; аппаратные средства; конфигурирование; аудит.
3	Мониторинг и оперативное управление	Мониторинг и оперативное управление; полномочное управление доступом и контроль печати.
4	Централизованная инвентаризация ресурсов локальной сети	Централизованная инвентаризация ресурсов локальной сети; удаленный контроль работоспособности средств защиты информации на рабочих станциях.
5	Инспекции в автоматизированных системах	Подготовка к инспекциям; инспекции компьютеров; получение отчетов с результатами инспектирования.
6	Централизованная защита от вирусов в локальной сети	Централизованная защита от вирусов в локальной сети
7	Управление системой безопасности автоматизированной системы	Управление серверами администрирования; управление группами администрирования; управление клиентскими компьютерами, работа с отчетами, статистикой.
8	Централизованный учет и управление программно-аппаратными средствами защиты информации	Централизованный учет и управление программно- аппаратными средствами защиты информации.
9	Управление жизненным циклом и аудит средств аутентификации	Управление жизненным циклом средств аутентификации; аудит использования средств аутентификации
10	Нормативные требования по управлению средствами защиты информации	Анализ нормативных требований по управлению средствами защиты информации; нормативные требования ФСТЭК при обеспечении мер безопасности персональных данных, в государственных информационных системах;

		требования безопасности к автоматизированным системам управления технологическими процессами.

5.2. Практические занятия

Наименование темы	Содержание темы
Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети	Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети
Основные механизмы защиты	Основные механизмы защиты
Мониторинг и оперативное управление	Мониторинг и оперативное управление
Централизованная инвентаризация ресурсов локальной сети	Централизованная инвентаризация ресурсов локальной сети

5.3. Лабораторные занятия

Наименование темы	Содержание темы
Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети	Разграничение доступа к данным. Разграничение доступа к устройствам. Контроль печати конфиденциальных данных.
Основные механизмы защиты	Замкнутая программная среда. Контроль целостности.
Мониторинг и оперативное управление	Аудит событий информационной безопасности в КСЗИ. Работа со сведениями в журнале регистрации событий. Теневое копирование.
Централизованная инвентаризация ресурсов локальной сети	Инвентаризация аппаратного и программного обеспечения в локальной сети.
Инспекции в автоматизированных системах	Проведение инспекций и учет изменений конфигурации защищаемых рабочих станций.
Централизованная защита от вирусов в локальной сети	Администрирование системы антивирусной защиты в локальной сети.
Управление жизненным циклом и аудит средств аутентификации	Управление жизненным циклом средств аутентификации.

6. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)	Трудоемкость в академических часах
1	Централизованное управление средствами защиты информации от несанкционированного доступа в	Повторение лекционного материала. Изучение учебной литературы. Подготовка к практической работе. Выполнение лабораторной работы.	5.8

	локальной сети		
2	Основные механизмы защиты	Повторение лекционного материала. Изучение учебной литературы. Подготовка к практической работе. Выполнение лабораторной работы.	6
3	Мониторинг и оперативное управление	Повторение лекционного материала. Изучение учебной литературы. Подготовка к практической работе. Выполнение лабораторной работы.	6
4	Централизованная инвентаризация ресурсов локальной сети	Повторение лекционного материала. Изучение учебной литературы. Подготовка к практической работе. Выполнение лабораторной работы.	6
5	Инспекции в автоматизированных системах	Повторение лекционного материала. Изучение учебной литературы. Подготовка к лабораторной работе. Выполнение лабораторной работы.	6
6	Централизованная защита от вирусов в локальной сети	Повторение лекционного материала. Изучение учебной литературы. Подготовка к лабораторной работе. Выполнение лабораторной работы.	6
7	Управление системой безопасности автоматизированной системы	Повторение лекционного материала. Изучение учебной литературы.	6
8	Централизованный учет и управление программно-аппаратными средствами защиты информации	Повторение лекционного материала. Изучение учебной литературы.	6
9	Управление жизненным циклом и аудит средств аутентификации	Повторение лекционного материала. Изучение учебной литературы. Подготовка к лабораторной работе. Выполнение лабораторной работы.	6
10	Нормативные требования по управлению средствами защиты информации	Повторение лекционного материала. Изучение учебной литературы.	8

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательный процесс по дисциплине строится на основе комбинации следующих образовательных технологий.

Интегральную модель образовательного процесса по дисциплине формируют технологии методологического уровня: модульно- рейтинговое обучение, технология поэтапного формирования умственных действий, технология развивающего обучения, элементы технологии развития критического мышления.

Реализация данной модели предполагает использование следующих технологий стратегического уровня (задающих организационные формы взаимодействия субъектов образовательного процесса), осуществляемых с использованием определенных тактических процедур:

– лекционные (вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция);
– лабораторные (углубление знаний, полученных на теоретических занятиях, решение задач);
– практические (формирование определенных умений и навыков, формирование алгоритмического мышления);
– активизации познавательной деятельности (приемы технологии развития критического мышления через чтение и письмо, работа с литературой, подготовка презентаций по темам домашних работ);
– самоуправления (самостоятельная работа студентов, самостоятельное изучение материала).
Информационные технологии используются при организации коммуникации со студентами для представления информации, выдачи рекомендаций и консультирования по оперативным вопросам (электронная почта), использование мультимедиа-средств при проведении лекционных и практических занятий.
В качестве образовательных технологий при изучении дисциплины используются, мультимедийные лекции, на лабораторных занятиях используются лабораторные стенды и современные пакеты программных продуктов. С целью текущего контроля знаний студентов на лабораторных работах проводится контроль выполнения работы. Студентам предлагается обсудить поученные результаты и высказать свое мнение по применению возможных приемов для улучшения показателей либо результатов работы.

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Промежуточная аттестация (7 семестр): зачёт.
Вопросы для подготовки к зачету:
1. Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети.
2. Принципы построения комплексных систем защиты информации (КСЗИ).
3. Основные механизмы защиты.
4. Аппаратные средства защиты; конфигурирование; аудит.
5. Мониторинг и оперативное управление.
6. Полномочное управление доступом и контроль печати.
7.Централизованная инвентаризация ресурсов локальной сети.
Промежуточная аттестация по итогам освоения дисциплины (8 семестр): экзамен.
Вопросы для подготовки к экзамену.
1. Удаленный контроль работоспособности средств защиты информации на рабочих станциях.
2. Подготовка к инспекциям; инспекции компьютеров.
3. Получение отчетов с результатами инспектирования.
4. Централизованная защита от вирусов в локальной сети.
5. Управление серверами администрирования.
6. Управление группами администрирования.
7. Управление клиентскими компьютерами.
8. Работа с отчетами, статистикой.
9. Централизованный учет и управление программно- аппаратными средствами защиты информации.
10. Управление жизненным циклом средств аутентификации.
11. Аудит использования средств аутентификации.
12. Анализ нормативных требований по управлению средствами защиты информации.
13. Нормативные требования ФСТЭК при обеспечении мер безопасности персональных данных, в государственных информационных системах.
14. Требования безопасности к автоматизированным системам управления технологическими процессами.

9. УЧЕБНО- МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

УЧЕБНОГО ПРЕДМЕТА

а) литература

1. Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно- библиотечная система. — URL: https:// e.lanbook.com/book/163844 (дата обращения: 21.03.2024).
2. 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: 21.03.2024).
3. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш [и др.]. — Ставрополь : Северо- Кавказский федеральный университет, 2016. — 242 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/62945.html (дата обращения: 21.03.2024).
4. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https:// www.iprbookshop.ru/108227.html (дата обращения: 21.03.2024).
5. Чуянов, А. Г. Обеспечение информационной безопасности в компьютерных системах : учебное пособие / А. Г. Чуянов, А. А. Симаков. — Омск : Омская академия МВД России, 2012. — 204 с. — ISBN 978-5-88651-535-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https:// www.iprbookshop.ru/36015.html (дата обращения: 21.03.2024).
6. Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации : учебное пособие / О. М. Голембиовская, М. Ю. Рытов, К. Е. Шинаков [и др.]. — 2-е изд. — Саратов : Вузовское образование, 2024. — 265 с. — ISBN 978-5-4487-0942-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/134999.html (дата обращения: 21.03.2024).

б) программное обеспечение и Интернет-ресурсы

№	Наименование	Описание
1	Операционная система Linux	GNU-лицензия (GNU General Public License)
2	Max Patrol Education	Лицензионный договор № 003-17/ЕМ.
3	Secret Net 6	Сублицензионный договор №34/02/ ИБиИТ/697 от 09.08.2013.
4	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.
5	Страж-NT	Сублицензионный договор №34/02/ ИБиИТ/697 от 09.08.2013.
6	http://www.IPRbooks.ru	Электронная библиотечная система «IPRbooks» специализируется на учебных материалах по гуманитарным, естественным и точным наукам
7	https://e.lanbook.com/	ЭБС «Лань» – это крупнейшая политематическая база данных, включающая в себя контент сотен издательств

		научной, учебной литературы и научной периодики.
8	https://urait.ru	Образовательная платформа Юрайт – образовательный ресурс, электронная библиотека и интернет-магазин, где читают и покупают электронные и печатные учебники авторов – преподавателей ведущих университетов для всех уровней профессионального образования, а также пользуются видео- и аудиоматериалами, тестированием и сервисами для преподавателей, доступными 24 часа 7 дней в неделю

в) профессиональные базы данных и информационные справочные системы

№	Наименование	Описание
1	www.elibrary.ru	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.
2	https://fstec.ru/	Официальный сайт Федеральной службы по техническому и экспортному контролю

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.