МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»
Институт информационных технологий, машиностроения и автотранспорта

УТВЕРЖДАЮ
Директор ИИТМА
_____ Д.В. Стенин
«____»_____ 20__ г.

Рабочая программа дисциплины

Информационная безопасность и защита информации

Направление подготовки 09.03.02 Информационные системы и технологии
Направленность (профиль) 01 Системная интеграция и автоматизация информационных процессов

Присваиваемая квалификация
"Бакалавр"

Формы обучения
очная

Кемерово 2021 г.

Рабочую программу составил:
Старший преподаватель кафедры ИиАПС С.А. Асанов

Рабочая программа обсуждена
на заседании кафедры информационных и автоматизированных производственных систем

Протокол № _____ от _____

Зав. кафедрой информационных и автоматизированных производственных систем _____ И.В. Чичерин

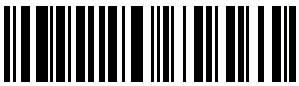
подпись ФИО

Согласовано учебно-методической комиссией
по направлению подготовки (специальности) 09.03.02 Информационные системы и технологии

Протокол № _____ от _____

Председатель учебно-методической комиссии по направлению подготовки (специальности) 09.03.02 Информационные системы и технологии _____ И.В. Чичерин

подпись ФИО


1621623957

1 Перечень планируемых результатов обучения по дисциплине "Информационная безопасность и защита информации", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

профессиональных компетенций:

ПК-11 - Восстановление работоспособности программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих после сбоев

ПК-12 - Протоколирование событий, возникающих в процессе работы инфокоммуникационной системы

ПК-2 - Оценка критичности возникновения инцидентов при работе прикладного программного обеспечения

ПК-5 - Реализация регламентов обеспечения информационной безопасности прикладного программного обеспечения

ПК-6 - Разработка нормативно-технической документации на процедуры управления прикладным программным обеспечением

ПК-9 - Управление доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

выполняет фильтрацию протоколов информационной системы по уровню критичности;

- владеет навыками поиска информации в сети Интернет по кодам ошибок;

применяет программное обеспечение тестирования конфигурации компонентов защиты в рамках информационной системы;

использует программное обеспечение постановки и контроля задач для подготовки алгоритмов управления программным обеспечением;

настраивает права доступа к объектам информационной системы;

- управляет субъектами доступа информационной системы;

выполняет запуск средств аварийного восстановления с помощью встроенных средств информационной системы;

- выполняет запуск средств аварийного восстановления с внешнего носителя;

выполняет настройку средств протоколирования событий по заданным параметрам;

Результаты обучения по дисциплине:

основы организационного и правового обеспечения информационной безопасности;

-

основные нормативные правовые акты в области обеспечения информационной безопасности;

-

каналы утечки информации, возможности технических средств перехвата информации; основные средства и способы обеспечения информационной безопасности;

-

задачи органов защиты государственной тайны и служб информационной безопасности на предприятиях;

- наиболее рациональные способы защиты и порядок действий коллектива предприятия в чрезвычайных ситуациях;

основы государственной информационной политики;

-

основы информационной безопасности и защиты информации;

-

классифицировать и оценивать угрозы информационной безопасности;

-

осуществлять обоснованный выбор средств и систем защиты информации;

-

классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

разрабатывать политики информационной безопасности;

- эффективно применять средства защиты от негативных воздействий;

применять нормативные правовые акты в области обеспечения информационной безопасности;

-

анализировать безопасность функционирования инфотелекоммуникационных систем;

-

навыками применения технических средств защиты информации;
-
методами контроля за исполнением политик информационной безопасности;
-
методами повышения безопасности технических средств и технологических процессов;
профессиональной терминологией в области информационной безопасности;
владеть навыками работы с нормативными правовыми актами;
-
методиками анализа предметной области;
-

2 Место дисциплины "Информационная безопасность и защита информации" в структуре ОПОП бакалавриата

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Информатика, Информационные технологии, Инфокоммуникационные системы и сети, Компьютерные технологии в автоматизации деятельности предприятий, Управление IT-проектами.

Целями освоения дисциплины являются:
- изучение основных понятий и составляющих информационной безопасности;
- изучение принципов организации и алгоритмов обеспечения безопасности информационных систем и пользовательских данных;
- освоение современных средств обеспечения информационной безопасности;
- развитие навыков применения системного программного обеспечения и пакетов прикладных программ для решения практических задач по профилю дисциплины.

3 Объем дисциплины "Информационная безопасность и защита информации" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Информационная безопасность и защита информации" составляет 4 зачетных единицы, 144 часа.

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 4/Семестр 8			
Всего часов	144		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции	16		
Лабораторные занятия	32		
Практические занятия			
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа	60		
Форма промежуточной аттестации	экзамен /36		

4 Содержание дисциплины "Информационная безопасность и защита информации", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах		
	ОФ	ЗФ	ОЗФ

РАЗДЕЛ 1. ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Общая проблема информационной безопасности. Критерии оценки защищенности информационных систем.	1		
РАЗДЕЛ 1. ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Доктрина информационной безопасности России	1		
РАЗДЕЛ 1. ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Организационные вопросы разграничения доступа к информации. Политики паролей. Социальная инженерия как средство получения несанкционированного доступа к информации.	3		
РАЗДЕЛ 2. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. Физический уровень защиты как первая ступень обороны. Средства физической зашиты.	1		
РАЗДЕЛ 2. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. Защита информации с помощью аппаратных средств при реализации основных информационных процессов (ввод, вывод, передача, обработка, накопление, хранение). Виртуальные частные сети.	2		
РАЗДЕЛ 2. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИю Шифрование данных как метод защиты информации. Системы шифрования с симметричными (секретными) ключами. Системы шифрования с открытыми ключами.	2		
РАЗДЕЛ 2. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. Файловые системы, обеспечивающие защиту информации. Утилиты сжатия и шифрования данных. Межсетевые экраны как средство разграничения доступа к информации. Механизмы защиты протоколов связи. Протоколы аутентификации. Цифровые сертификаты и подписи. Протокол Kerberos и инициатива Single Sign-On.	6		

4.2. Лабораторные занятия

Наименование работы	Трудоемкость в часах		
	ОФ	ЗФ	ОЗФ
Компьютерные вирусы	4		
Конфигурирование межсетевых экранов	6		
Виртуальные частные сети	4		
Методы сканирования портов	4		
Анализ сетевого трафика	4		
Аудит систем аутентификации	6		
Контроль целостности данных	4		

4.3 Практические (семинарские) занятия

Тема занятия	Трудоемкость в часах		
	ОФ	ЗФ	ОЗФ

4.4 Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Вид СРС	Трудоемкость в часах		
	ОФ	ЗФ	ОЗФ
Изучение литературы согласно темам разделов дисциплины	20		
Оформление отчетов по лабораторным работам	60		
Защита отчетов по лабораторным работам	12		

4.5 Курсовое проектирование

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Информационная безопасность и защита информации"

5.1 Паспорт фонда оценочных средств

№	Наименование разделов дисциплины	Содержание (темы) раздела	Код компетенции	Знания, умения, навыки, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, навыков, необходимых для формирования соответствующей компетенции

5.2. Типовые контрольные задания или иные материалы

5.2.1.Оценочные средства при текущем контроле

Текущий контроль по дисциплине заключается в опросе обучающихся по контрольным вопросам, в оформлении и защите отчетов по лабораторным работам.

Опрос по контрольным вопросам

При проведении текущего контроля обучающимся письменно задаётся два вопроса, на которые они должны дать ответы.

Например: 1) дайте определение конфиденциальности информации; 2) перечислите основные угрозы информационной безопасности;

Критерии оценивания:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 75–99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 50–74 баллов - при правильном и неполном ответе на два вопроса или правильном и полном ответе только на один из вопросов;
- 25–49 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов 0-24 25-49 50-74 75-99 100

Шкала оценивания Не зачтено Зачтено

Отчет по лабораторным работам

По каждой работе студенты самостоятельно оформляют отчеты на бумажном носителе в рукописном виде. Отчет должен содержать:

1. Тему лабораторной работы.
2. Цель работы.
3. Вариант задания.
4. Описание выполненных действий.

1621623957

5. Результаты выполненных расчетов (для расчетных заданий). 6. Анализ полученных результатов.
7. Вывод.

Критерии оценивания:

1 балл - при раскрытии всех разделов в полном объеме;

0 баллов - при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов 0 1

Шкала оценивания Не зачтено Зачтено

Защита отчетов по лабораторным работам

Оценочными средствами для текущего контроля по защите отчетов являются контрольные вопросы к лабораторным работам. При проведении текущего контроля обучающимся будет письменно задано два вопроса, на которые они должны дать ответы. Например: 1) Что называется компьютерным вирусом? 2) Какие вирусы называются резидентными?

Критерии оценивания:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 75–99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 50–74 баллов - при правильном и неполном ответе на два вопроса или правильном и полном ответе только на один из вопросов;
- 25–49 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов 0-24 25-49 50-74 75-99 100

Шкала оценивания Не зачтено Зачтено

5.2.2 Оценочные средства при промежуточной аттестации

Формой промежуточной аттестации является экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций. Инструментом измерения сформированности компетенций являются оформленные и зачтенные отчеты по лабораторным работам, ответы на вопросы во время опроса по темам лекций, экзаменационные вопросы.

На экзамене обучающийся отвечает на билет, в котором содержится 2 вопроса и задача. Оценка за экзамен выставляется с учетом отчетов по лабораторным работам и ответа на вопросы.

Критерии оценивания для экзамена:

- 100 баллов – при правильно решенной задаче и правильном и полном ответе на два вопроса;
- 75–99 баллов – при правильно решенной задаче и правильном и полном ответе на один из вопросов и правильном, но не полном
ответе на другой из вопросов;
- 50–74 баллов - при правильно решенной задаче и правильном и неполном ответе на два вопроса или правильном и полном ответе
только на один из вопросов;
- 25–49 баллов – при правильно решенной задаче и правильном и неполном ответе только на один из вопросов;
- 0–24 баллов – при отсутствии правильных ответов на вопросы или при неправильно решенной задаче.

Количество баллов 0-64 65-79 80-90 90-100 Шкала оценивания НЕУД УДОВЛ ХОР ОТЛ

Примерный перечень вопросов для экзамена:

1. Основные определения информационной безопасности: информация, автоматизированная система обработки информации, информационная безопасность, конфиденциальность, целостность и доступность информации, угроза информационной безопасности, виды угроз.
2. Уровни доступа к информации в системе обработки информации и структуризация методов обеспечения информационной безопасности.
3. Основные направления реализации угроз информационной безопасности.
4. Основные методы реализации угроз информационной безопасности.
5. Основные принципы обеспечения информационной безопасности.
6. Основные направления обеспечения информационной безопасности.
7. Основные критерии оценки защищенности информационных систем.
8. Правовая защита информации. Понятие коммерческой тайны.
9. Организационная защита информации. Основные задачи службы безопасности предприятия.
10. Инженерно-техническая защита информации. Физические методы инженерно-технической защиты информации.
11. Аппаратные средства инженерно-технической защиты информации.
12. Программные средства инженерно-технической защиты информации.

5.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

При проведении текущего контроля по темам в конце занятия обучающиеся убирают все личные вещи с учебной мебели, достают листок чистой бумаги и ручку. На листке бумаги записываются Фамилия, Имя, Отчество, номер группы и дата проведения опроса. Далее преподаватель задает два вопроса в устной форме. В течение пяти минут обучающиеся должны дать ответы на заданные вопросы, при этом использовать любую печатную и рукописную продукцию, а также любые технические средства не допускается. По истечении указанного времени листы с ответами сдаются преподавателю на проверку. Результаты оценивания ответов на вопросы доводятся до сведения обучающихся не позднее семи учебных дней после даты проведения опроса.

Если обучающийся воспользовался любой печатной или рукописной продукцией, а также любыми техническими средствами, то его ответы на вопросы не принимаются и ему выставляется 0 баллов.

При проведении текущего контроля по лабораторным работам обучающиеся представляют отчет по лабораторной работе преподавателю. Преподаватель анализирует содержание отчетов, после чего оценивает достигнутый результат.

До промежуточной аттестации допускается студент, который выполнил все требования текущего контроля.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для студентов вузов, обучающихся по специальности "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 5-е изд., стер. – Москва : Академия, 2011. – 336 с. – (Высшее профессиональное образование : Информатика и вычислительная техника). – Текст : непосредственный.

2. Шаньгин, В. Ф. Защита компьютерной информации / В. Ф. Шаньгин. – Москва : ДМК Пресс, 2010. – 544 с. – ISBN 9785940745181. – URL: http://biblioclub.ru/index.php?page=book_red&id=86475 (дата обращения: 17.05.2022). – Текст : электронный.

3. Петров, А. А. Компьютерная безопасность / А. А. Петров. – Москва : ДМК Пресс, 2008. – 448 с. – ISBN 5898180648. – URL: http://biblioclub.ru/index.php?page=book_red&id=232067 (дата обращения: 17.05.2022). – Текст : электронный.

6.2 Дополнительная литература

1. Ярочкин, В. И. Информационная безопасность : учебник для студентов вузов / В. И. Ярочкин. – Москва : Академический проект, 2005. – 544 с. – (Учебник для вузов). – Текст : непосредственный.

2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учеб. пособие для студентов вузов, обучающихся по специальностям, не входящим в группу специальностей в области информ. безопасности / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. – 3-е изд., стер. – Москва : Горячая линия-Телеком, 2005. – 147 с. – Текст : непосредственный.

3. Лапонина, О. Р. Межсетевые экраны / О. Р. Лапонина. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 466 с. – URL: http://biblioclub.ru/index.php?page=book_red&id=429093 (дата обращения: 17.05.2022). – Текст : электронный.

6.3 Методическая литература

6.4 Профессиональные базы данных и информационные справочные системы

1. Электронная библиотека КузГТУ https://elib.kuzstu.ru/index.php?option=com_content&view=article&id=230&Itemid=229

6.5 Периодические издания

1. Вестник Кузбасского государственного технического университета : научно-технический журнал (печатный/электронный) https://vestnik.kuzstu.ru/

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. ЭБС "Университетская библиотека онлайн" читать электронные книги [Электронный ресурс] — Режим доступа: http://biblioclub.ru/

2. Основы информационной безопасности [Электронный ресурс] — Режим доступа: http://www.intuit.ru/studies/courses/10/10/info

3. Межсетевые экраны [Электронный ресурс] — Режим доступа: http://www.intuit.ru/studies/courses/14250/1286/info

8 Методические указания для обучающихся по освоению дисциплины "Информационная безопасность и защита информации"

Основной учебной работой студента является самостоятельная работа в течение всего срока обучения. Начинать изучение дисциплины необходимо с ознакомления с целями дисциплины, знаниями и умениями, приобретаемыми в процессе изучения. Далее следует проработать конспекты лекций, рассмотрев отдельные вопросы по предложенным источникам литературы. Все вопросы по дисциплине студент может разрешить на консультациях, проводимых по расписанию.

При подготовке к лабораторным занятиям студент в обязательном порядке изучает теоретический материал в соответствии с методическими указаниями к лабораторным занятиям.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Информационная безопасность и защита информации", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:
1. Ubuntu
2. Libre Office
3. Mozilla Firefox
4. Microsoft Windows

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Информационная безопасность и защита информации"

Для осуществления образовательного процесса по данной дисциплине необходима следующая материально-техническая база:

- лекционная аудитория;
- учебная аудитория, оснащенная вычислительной техникой по количеству обучающихся в группе (подгруппе), для проведения лабораторных занятий;
- научно-техническая библиотека для самостоятельной работы обучающихся;
- зал электронных ресурсов КузГТУ с выходом в сеть «Интернет» для самостоятельной работы обучающихся;
- учебная аудитория, оснащенная вычислительной техникой, для самостоятельной работы обучающихся.

11 Иные сведения и (или) материалы

Учебная работа проводится с использованием как традиционных так и современных интерактивных технологий. В рамках занятий применяются следующие интерактивные методы:

– разбор конкретных примеров;
– творческое задание;
– беседа с приглашенным специалистом;
– мультимедийная презентация.