Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Первый проректор
_____ / Т.Р. Змызгова/
«__» сентября 2021 г.

Рабочая программа учебной дисциплины

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

образовательной программы высшего образования –
программы бакалавриата

15.03.04 Автоматизация технологических процессов и производств

Направленность: Автоматизация технологических процессов и производств (в машиностроении)
Форма обучения: очная, , заочная

Курган 2021

представлена пояснительная записка. Рекомендуемая структура пояснительной записки:

- титульный лист
- информационная часть
- введение
- основная часть
- заключение
- список использованных источников

Примерные темы контрольных работ

1. Угрозы безопасности информационной системе.
2. Организационные и физические меры защиты информации.
3. Биометрические средства ограничения доступа.
4. Пластиковые карты.
5. Кодирование и перекодирование информации.
6. Пароли.
7. Защита документов, подготовленных в текстовом редакторе Ms Word.
8. Защита документов, подготовленных в табличном процессоре Excel.
9. Защита html-документов и веб-сайтов.
10. Защита исполняемых программ.
11. Защита носителей информации.
12. Сетевые атаки и организация защиты в сети.
13. Электронная подпись и защита электронных сделок.
14. Защита персональных данных.
15. Основные приемы безопасной работы на компьютере.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной работе.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале лабораторной работы.

Преподавателем запланировано применение на лабораторных работах технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (зачету) набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных лабораторных работ. Формы дополнительных заданий (назначаются преподавателем): - выполнение и защита пропущенной лабораторной работы (при невозможности дополнительного проведения лабораторной работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 7 баллов. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий состоят для 1 и 2 рубежного контроля из 13 вопросов. На каждое тестирование при рубежном контроле студенту отводится 1 академический час.

Баллы студенту выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%
«удовлетворительно» – 50% - 70%
«хорошо» – 70% - 90%
«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты тестирования каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Зачет проводится в форме ответов на вопросы билета. Билет состоит из 2 вопросов. Вопросы к зачету доводятся до студентов на последней лекции в семестре. На подготовку ответа студенту отводится 1 астрономический час. Каждый вопрос оценивается до 15 баллов.

Результаты успеваемости и зачета заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежного контроля и зачета

1-ый рубежный контроль

Вопрос 1. Доступ к информации, не нарушающий правила разграничения доступа, называется…

а) легальным;

б) нелегальным;

в) санкционированным;

г) вредоносным;

д) несанкционированным.

Вопрос 2. Субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на множество субъектов, имеющих доступ к данной информации

а) целостность;

б) доступность;

в) конфиденциальность;

г) своевременность.

Вопрос 3. Уязвимость информации — это:

а) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

б) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

в) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

2-ой рубежный контроль

Вопрос 1. К не преднамеренным угрозам относятся:

а) ошибки в разработке программных средств КС;

б) несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями;

в) угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой.

Вопрос 2. При парольной защите в качестве аутентификационного фактора субъекта выступает

а) то, что он знает;

б) то, чем он владеет;

в) то, что есть часть его самого.

Вопрос 3. Основные направления обеспечения КБ в зависимости от природы средств и методов:

а) компьютерное, криптографическое, бумажное

б) нормативное, формальное, практическое (экспериментальное)

в) нормативно-правовое, инженерно-техническое, организационное, аппаратно-программное

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Информация как объект защиты. Конфиденциальность, целостность и доступность информации.
2. Модели ценности информации. Информационный поток.
3. Иерархические модели и модель взаимодействия открытых систем (OSI/ISO).
4. Угрозы. Классификация угроз безопасности.
5. Модели угроз и модель нарушителя.
6. Утечки информации. Каналы утечек информации.
7. Классификация каналов утечек информации.
8. Основные направления обеспечения компьютерной безопасности.
9. Основные уровни защиты информации.
10. Принципы построения безопасных АС. Методология обследования и проектирования защиты АС.
11. Системы идентификации и аутентификации, классификация таких систем. Криптографические средства защиты информации.
12. Стеганографические методы защиты.
13. Контроль целостности информации на МНИ.
14. Цифровая подпись.
15. Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак.
16. Средства реализации атак.
17. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.
18. Технологии обнаружения компьютерных атак и их возможности.
19. Методы обнаружения атак. Классификация систем обнаружения атак /вторжений (СОА/СОВ).
20. Вредоносное программное обеспечение.
21. Компьютерные вирусы. Классификация вирусов.
22. Антивирусное программное обеспечение. Классификация антивирусов.
23. Требования к антивирусным программам. Методы обнаружения вредоносного ПО и устранения последствий заражения.
24. Понятие межсетевого экрана. Стратегии и средства межсетевого экранирования.
25. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов.
26. Типы межсетевых экранов. Схемы межсетевого экранирования.
27. Фильтрация пакетов. Критерии и правила фильтрации.
28. Реализация пакетных фильтров. Особенности фильтрации различных типов трафика.

29. Шлюзы прикладного уровня. Контроль HTTP-трафика и электронной почты.

30. Понятие виртуальной частной сети, ее предназначение. Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.

31. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации.

32. Защита данных на сетевом уровне. Защищенный обмен электронной почтой.

33. Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ.

34. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем.

35. Определение структуры информационно-телекоммуникационных сетей.

36. Программные средства анализа топологии вычислительной сети.

37. Определение маршрутов прохождения сетевых пакетов.

38. Обнаружение объектов сети. Построение схемы сети.

39. Выявление телекоммуникационного оборудования.

40. Выявление и построение схемы информационных потоков защищаемой информации.

41. Понятие политики безопасности. Основные типы политики безопасности.

42. Разработка и реализация политики безопасности. Классификация моделей политик безопасности.

43. Политика и модели безопасности в распределенных компьютерных системах.

44. Семейство ДП-моделей политик безопасности логического управления доступом и информационными потоками.

45. Основные критерии оценки защищенности АС.

46. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»).

47. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.

48. Единые критерии безопасности информационных технологий (Common Criteria).

49. Определение уровня защищённости и требования по защите персональных данных.

50. Требования по защите КИИ.

6.5. Фонд оценочных средств

Полный банк заданий для текущего контроля и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

7.1.1. Основная литература:

1. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. – М.: «Академия», 2009. - 272 с.

2. Галатенко, В.А. Основы информационной безопасности. / [Электронный ресурс]. - М.: Национальный Открытый Университет "ИНТУИТ", 2016 - 208 с. ISBN 5-9556-0052-3. - Доступ ЭБС «Консультант студента».

3. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] - Москва: ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0. - Доступ ЭБС «Консультант студента».

4. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие для вузов 2-е изд., испр. и доп. [Электронный ресурс] - Москва: Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9. - Доступ ЭБС «Консультант студента».

7.1.2. Дополнительная литература:

1. Касперски, К. Техника сетевых атак. Т. 1 / Крис Касперски. – М.: Солон-Р, 2001. – 400 с.

2. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций: учебное пособие: для студентов вузов, обучающихся по специальности 510200 "Прикладная математика и информатика"/ О.Р. Лапонина; Интернет-университет информационных технологий. – М.: Интернет-Университет информационных технологий, 2005. – 605 с.

3. Олифер, В.Г. Компьютерные сети: Принципы, технологии, протоколы: учебное пособие для студентов вузов / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – М.; СПб.; Нижний Новгород: Питер, 2007. – 957, с.

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Электронный фонд правовой и нормативно-технической документации - http://docs.cntd.ru;
2. ЭБС «Лань» - https://e.lanbook.com/;
3. ЭБС «Znanium» - https://znanium.com/;
4. ЭБС «Консультант студента» - https://www.studentlibrary.ru;
5. Национальный Открытый Университет «ИНТУИТ» - https://intuit.ru;
6. Единое окно доступа к образовательным ресурсам. – http://window.edu.ru/;
7. Научная электронная библиотека - http://elibrary.ru/;
8. Электронная библиотека КГУ - http://dspace.kgsu.ru/xmlui/;
9. Информационный онлайн портал ISO27000.ru - http://www.iso27000.ru/;

10. Безопасность - http://groteck.ru/security.

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

Система KESS поддержки образовательного процесса КГУ http://dist.kgsu.ru/.

При чтении лекций используются слайдовые презентации.

Программные средства обеспечения учебного процесса включают в себя: базовые (операционные системы (Windows); инструментальные средства программирования), вспомогательные (программы презентационной графики; текстовые редакторы; графические редакторы).

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины включает в себя учебные аудитории и лаборатории, оснащенные проекционным оборудованием с экраном, современными компьютерами (все – в стандартной комплектации для практических занятий и самостоятельной работы), объединенными локальными вычислительными сетями с выходом в Интернет. Обучающемуся предоставляется возможность практической работы.

В соответствии с ООП дисциплина поддерживается соответствующими лицензионными программными продуктами.

При использовании электронных изданий вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет.

11. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений, обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Защита информации в компьютерных системах»

образовательной программы высшего образования –
программы бакалавриата

15.03.04 – Автоматизация технологических процессов и производств

Направленность: **Автоматизация технологических процессов и производств (в машиностроении)**

Трудоемкость дисциплины: 3 з.е. (108 академических часа – очная и заочная формы обучения)

Семестр: 3 (очная форма обучения)

Семестр: 4 (заочная форма обучения)

Форма промежуточной аттестации: зачет

Содержание дисциплины. Основные разделы.

Информация как объект защиты. Информационная безопасность. Аппаратно-программные средства защиты информации. Критерии оценки безопасности компьютерных систем. Криптографические средства защиты информации. Защита от несанкционированного доступа. Типовые угрозы информационной безопасности. Технологии обеспечения безопасности в компьютерных сетях.