МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «СГУ имени Н.Г. Чернышевского»

Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ

«13» 01 2017 г.

Рабочая программа дисциплины

Технические средства защиты информации

Специальность

10.05.01 Компьютерная безопасность

Специализация

Математические методы защиты информации

Квалификация выпускника

Специалист по защите информации

Форма обучения

Очная

Саратов,

2017

1. Цели освоения дисциплины

Целями освоения дисциплины «Технические средства защиты информации» являются: закрепление теоретических знаний, полученных в ходе изучения дисциплин на 1-3 курсах; освоение и систематизация знаний, относящихся к средствам защиты информации; приобретение опыта работы с техническими средствами защиты компьютерной информации.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к вариативной части ФТД.Факультативы ООП и направлена на формирование у обучающихся общепрофессиональных и профессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Языки программирования», «Аппаратные средства вычислительной техники», «Основы информационной безопасности».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен обладать следующими профессиональными компетенциями:

- способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-6);
- способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности (ПК-1);
- способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований (ПК-2).

В рамках указанных компетенций обучающийся должен

- Знать:

– основные средства и методы анализа программных реализации;

- Уметь:

– грамотно пользоваться языком предметной области;

– формализовать задачу и разработать эффективный алгоритм ее решения;

- Владеть:

– техническими средствами защиты информации.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Всего часов	Лекции	Практические занятия	Самостоятельная работа	
1	2	3	4	5	6	7	8	9
1	Угрозы информационной безопасности	7	1-6	24	–	6	18	Опрос на 9–10-й неделе
2	Программно-аппаратные средства защиты информации		7-12	24	–	6	18	
3	Аппаратные средства защиты информации		13-18	24	–	6	18	
	Промежуточная аттестация							Зачёт с оценкой
	ИТОГО			**72**	**0**	**18**	**54**	**–**

Угрозы информационной безопасности. Классификация угроз информационной безопасности. Источники угроз информационной безопасности. Способы выявления угроз. Способы противодействия угрозам.

Программно-аппаратные средства защиты информации. Классификация средств защиты компьютерной информации. Программные средства защиты информации. Криптографические методы, стеганография. Антивирусное программное обеспечение. Сетевые экраны. Устройства защищенного хранения информации. Биометрические защиты. Разграничение доступа аппаратными методами. Создание и функционирование виртуальных частных сетей.

Аппаратные средства защиты информации. Технические каналы утечки информации: ПЭМИН, визуально-оптический, акустический (речевой), несанкционированный доступ к компьютерной информации и др. Краткая характеристика. Обзор технических средств негласного съёма информации. Методы и средства противодействия.

План практических занятий

На практических занятиях студенты выполняют задания, связанные с закреплением полученного теоретического материала, в том числе с использованием программного обеспечения.

№ занятия	Тема	Задания для практических занятий
1	**2**	**3**
1–3	Угрозы информационной безопасности	№№ 1-2
4–6	Программно-аппаратные средства защиты информации	№№ 3-5
7–9	Аппаратные средства защиты информации	№№ 6-8

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе таких активных и интерактивных форм проведения занятий как командное выполнение заданий, организация временных творческих коллективов, метод мозгового штурма, встречи с представителями российских компаний и государственных организаций, мастер-классы экспертов и специалистов.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве; увеличивается время на самостоятельное освоение материала.

Основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья и инвалидов, т. е. все студенты обучаются в смешанных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

В рамках самостоятельной работы студенты собирают и изучают методическую литературу (включая сетевые источники), необходимую для написания отчета по дисциплине. Каждый студент должен составить реферативный отчет по заданным темам.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для практических занятий, контрольные вопросы, темы отчётов (рефератов). Фонд оценочных средств дисциплины приведён в приложении 1.

7. Данные для учета успеваемости студентов в БАРС

Таблица 1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
7	0	0	60	20	0	0	20	100

Программа оценивания учебной деятельности студента

7 семестр

Лекции

Не предусмотрены.

Лабораторные занятия

Не предусмотрены.

Практические занятия

Оцениваются посещаемость, активность – от 0 до 40 баллов; самостоятельность при выполнении работы, грамотность в оформлении полученных результатов, правильность выполнения – от 0 до 20 баллов.

Самостоятельная работа

Оценивается качество выполненных работ, грамотность в оформлении – от 0 до 20 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Не предусмотрено.

Промежуточная аттестация

По окончанию дисциплины студент должен сдать преподавателю письменный отчет.

Аттестация проводится на основании оформленного в соответствии с установленными требованиями письменного отчета и, в случае необходимости, индивидуальную беседу с ним по результатам пройденной дисциплины. По итогам аттестации выставляется зачёт с оценкой.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 16 до 20 баллов;

ответ на «хорошо» оценивается от 11 до 15 баллов;

ответ на «удовлетворительно» оценивается от 6 до 10 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 5 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за седьмой семестр по дисциплине «Технические средства защиты информации» составляет 100 баллов.

Таблица 2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Технические средства защиты информации» в оценку (зачёт с оценкой)

80-100 баллов	«отлично» / зачтено
60-79 баллов	«хорошо» / зачтено
40-59 баллов	«удовлетворительно» / зачтено
0-39 баллов	«неудовлетворительно» / не зачтено

8. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1) Юрин, И. Ю. Теоретические и практические основы защиты информации [Электронный ресурс]: учеб. пособие / И. Ю. Юрин. Саратов, 2012. 32 с. URL: http://library.sgu.ru/uch_lit/620.pdf (дата обращения: 02.01.2017). Загл. с экрана. Яз. рус.

б) дополнительная литература:

1) Мельников, В. П. Информационная безопасность и защита информации [Текст] : учеб. пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - 4-е изд., стер. - Москва : Изд. центр "Академия", 2009. - 330, [6] с. : рис. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328 (36 назв.). - ISBN 978-5-7695-6150-4 (в пер.).

2) Ярочкин, В. И. Информационная безопасность [Текст] : учеб. для вузов / В. И. Ярочкин. - 5-е изд. - Москва : Акад. Проект, 2008. - 542, [2] с. : рис., табл. - (Gaudeamus). - Библиогр.: с. 534-539. - ISBN 978-5-8291-0987-5 (в пер.).

в) программное обеспечение:

1) Лицензионное программное обеспечение: Microsoft Windows; «КриптоПро».

2) Программно-аппаратный комплекс «Соболь»;

3) Программно-аппаратный комплекс «Аккорд»;

4) Программно-аппаратный комплекс «SecretNet»;

5) Аппаратные ключи «РуТокен»;

7) Зонд-монитор «СРМ-700»;

8) Нелинейный локатор «КАТРАН»;

9) Генератор шума «Гром ЗИ-4»;

10) Генератор шума «Гром ЗИ-6»;

11) Программно-аппаратный комплекс «ESMART Access Box»;

12) Биометрическая защита «EyeD OptiMouse».

9. Материально-техническое обеспечение дисциплины

Для проведения практических занятий необходим компьютерный класс с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом, оснащенный соответствующим программным обеспечением и аппаратным обеспечением.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность и специализации «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Автор

Старший преподаватель кафедры теоретических основ компьютерной безопасности и криптографии _____ И.Ю. Юрин

Программа разработана в 2012 г. (одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «25» мая 2012 года, протокол № 18).

Программа актуализирована в 2017 г. (одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «09» января 2017 года, протокол № 10).

Заведующий кафедрой теоретических основ компьютерной безопасности и криптографии, профессор, к.ф.-м.н. _____ В.Н. Салий

Декан факультета компьютерных наук и информационных технологий, к.ф.-м.н., доцент _____ А.Г. Федорова