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
Основы информационной безопасности

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 «Основы информационной безопасности» являются формирование базовых знаний в области обеспечения информационной безопасности, знакомство с предметной областью защиты информации, подготовка к изучению других профильных предметов.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к базовой части Блока 1 «Дисциплины (Модули)» ООП и направлена на формирование у обучающихся профессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Языки программирования», «Компьютерные сети», «Аппаратные средства вычислительной техники».

Компетенции, сформированные при изучении данной дисциплины, используются при изучении дисциплин «Защита в операционных системах», «Основы построения защищенных компьютерных сетей», «Основы построения защищенных баз данных», «Защита программ и данных», «Программно-аппаратные средства обеспечения информационной безопасности».

Компетенции, сформированные при изучении данной дисциплины, могут быть полезны при изучении дисциплин «Основы компьютерной экспертизы», «Криптографические методы защиты информации», «Техническая защита информации», «Введение в криптоанализ».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен обладать следующими компетенциями:

- 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 организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (ПК-13).

В рамках указанных компетенций обучающийся должен

- Знать:

– средства и методы хранения и передачи аутентификационной информации;

– требования к подсистеме аудита и политике аудита;

– источники и классификацию угроз информационной безопасности;

– основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;

• Уметь:

– анализировать и оценивать угрозы информационной безопасности объекта;

• Владеть:

– профессиональной терминологией в области информационной безопасности;

– методами формирования требований по защите 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	Лабораторные (Практические) занятия	Самостоятельная работа	
1	2	3	4	5	6	7	8	9
1	Теоретические основы защиты информации	5	1-4	16	8	–	8	Контрольная работа №1 на 18 неделе
2	Методы защиты информации		5-10	24	12	–	12	
3	Программные средства защиты информации		11-14	16	8	–	8	
4	Аппаратные средства защиты информации		15-18	16	8	–	8	
	Промежуточная аттестация							Зачет
	ИТОГО			**72**	**36**	–	**36**	–

Теоретические основы защиты информации. Основные определения. Угрозы информационной безопасности, их классификация. Разглашение, утечка, несанкционированный доступ к информации. Правила работы с машинными носителями информации. Формальные модели информационной безопасности. Модель политики контроля целостности. Модель Кларка-Вилсона. Идентификация и аутентификация. Виды парольных систем. Угрозы безопасности парольных систем. Атаки на парольные системы. Построение парольных систем.

Методы защиты информации. Использование контрольных сумм и хеширования для контроля целостности. Защита от разрушающих

программных воздействий. Алгоритмы работы антивирусных программ. Сокрытие информации. Стеганография.

Программные средства защиты информации. Защита программ от изучения. Защита программ от несанкционированного использования. Межсетевые экраны. Настройка виртуальных частных сетей.

Аппаратные средства защиты информации. Устройства для защищенного хранения информации. Электронные замки. Разграничение доступа с использованием программно-аппаратных средств. Биометрическая защита. Использование ГБШ для предотвращения утечки информации по техническим каналам.

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе таких активных и интерактивных форм проведения занятий как интерактивный опрос, эвристическая беседа, диалог, выступления экспертов и специалистов перед студентами, встречи с представителями ведущих отечественных фирм по защите информации, ознакомительные беседы с представителями потенциальных работодателей, экскурсия в музей регионального Управления ФСБ.

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 смешенных 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 изучают источники, в которых более детально рассматривается материал. Контроль текущей успеваемости осуществляется в процессе проведения лекционных занятий.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для контрольной работы, контрольные вопросы, вопросы для проведения промежуточной аттестации (зачет). 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
5	40	0	0	10	0	10	40	100

Программа оценивания учебной деятельности студента

5 семестр

Лекции

Посещаемость, активность за один семестр – от 0 до 40 баллов.

Лабораторные занятия

Не предусмотрены.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Качество выполнения заданий в рамках самостоятельной работы, грамотность оформления, глубина проработки материала – от 0 до 10 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Выполнение контрольной работы – от 0 до 10 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой зачет, проводимый в устной форме с предварительной подготовкой студента к ответу.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 31 до 40 баллов;

ответ на «хорошо» оценивается от 21 до 30 баллов;

ответ на «удовлетворительно» оценивается от 11 до 20 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 10 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за пятый семестр по дисциплине «Основы информационной безопасности» составляет 100 баллов.

Таблица 2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Основы информационной безопасности» в оценку (зачет)

35 баллов и более	«зачтено»
меньше 35 баллов	«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:

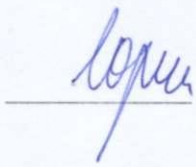
1) Корт, С. С. Теоретические основы защиты информации [Текст] : учеб. пособие / С. С. Корт. - Москва : Гелиос АРВ, 2004. - 233, [7] с. : ил. - Библиогр.: с. 226-229. - ISBN 5-85438-010-2.

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходима лекционная аудитория с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

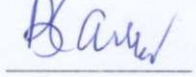
Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность и специализации «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

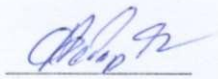
Автор

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