Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Амурский государственный университет»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ Н.В.Савина
«29» 06 2018 г.

РАБОЧАЯ ПРОГРАММА

Информационная безопасность

Направление подготовки 09.03.02 Информационные системы и технологии

Направленность (профиль) образовательной программы « Безопасность информационных систем»

Квалификация выпускника бакалавр

Программа подготовки академический бакалавриат

Год набора 2018

Форма обучения очная

Курс 2 Семестр 4

Зачет 4

Лекции 18 (акад. час.)

Практические занятия 18 (акад. час.)

Самостоятельная работа 36 (акад. час.)

Общая трудоемкость дисциплины 72 (акад. час.), 2 (з.е.)

Составитель Самохвалова С.Г. доцент кафедры ИУС, к.т.н

Факультет математики и информатики
Кафедра информационных и управляющих систем

2018г.

Рабочая программа составлена на основании Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.02 «Информационные системы и технологии», утвержденного приказом Министерства образования и науки 12.03.2015 г., № 219

Рабочая программа обсуждена на заседании кафедры информационных и управляющих систем

«_15_» _____05_____201_8_г., протокол №_9_

Заведующий кафедрой _____ А.В. Бушманов
подпись И.О.Ф.

Рабочая программа одобрена на заседании УМС направления подготовки 09.03.02 «Информационные системы и технологии»

«_29_» _____05_____201_8_г., протокол №9_

Председатель _____ А. В. Бушманов
подпись И.О.Ф.

СОГЛАСОВАНО
Начальник учебно-методического управления _____Н.А. Чалкина
(подпись)

«_29_» _____05_____20_18_ г.

СОГЛАСОВАНО
Заведующий выпускающей кафедрой _____А. В. Бушманов
(подпись)

«_15_» _____05_____20_18__ г.

СОГЛАСОВАНО
Директор научной библиотеки _____Л.А. Проказина
(подпись)

«_29_» _____05_____20_18_ г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины: заложить терминологический фундамент, рассмотреть основные общеметодологические принципы теории информационной безопасности; изучить методы и средства обеспечения ИБ, методы нарушения конфиденциальности, целостности и доступности информации и противодействия этим нарушениям.

Задачами дисциплины являются формирование знаний у студентов о современном состоянии проблемы обеспечения информационной безопасности при использовании компьютерных технологий, существующих угрозах, видах обеспечения информационной безопасности, методах и средствах защиты информации и основах построения комплексных систем защиты.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Информационная безопасность» входит в вариативную часть блока дисциплин, обеспечивая профессиональную подготовку по направлению «Информационные системы и технологии».

Данный курс базируется на знаниях, полученных в области информатики, проектирования и использования баз данных, операционных систем. Знания, умения и навыки, полученные в процессе изучения данного курса, могут быть использованы студентами при изучении дисциплин**,** «Защита информации в операционных системах», «Защита от утечки речевой информации», а также при выполнении ВКР.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Вместе с другими дисциплинами ОП дисциплина «Информационная безопасность» обеспечивает формирование следующих компетенций бакалавров:

способностью использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования (ОПК-2);

пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны (ОПК-4);

способностью проводить сбор, анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования (ПК-22);

способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ДПК-3).

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

Знать: принципы ИБ; основные угрозы информационной безопасности; сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны; методы и критерии оценки эффективности мероприятий по защите информации.

Уметь: различать правовые, организационные и технические мероприятия по защите информации; выявлять и классифицировать угрозы информационной безопасности предприятия; использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования; проводить сбор, анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования; планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия; рассчитывать эффективность мероприятий по защите информации

Владеть: современной терминологией и методологией в области информационной безопасности.

4. МАТРИЦА КОМПЕТЕНЦИЙ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы	Компетенции			
	ОПК - 2	ОПК-4	ПК-22	ДПК-3
Свойства информации как объекта защиты		+		
Актуальность проблемы обеспечения безопасности информации			+	
Угрозы информационной безопасности. Виды противников и каналы утечки информации.	+			
Вредоносное ПО. Компьютерные вирусы и средства защиты от них		+		+
Управление рисками			+	
Программно-технические методы защиты		+		+
Информационные войны и информационное оружие	+		+	

5.СТРУКТУРА ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 академических часа

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды контактной работы, включая самостоятельную работу студентов и трудоемкость (в академических часах)			Формы текущего контроля успеваемости Форма промежуточной аттестации
				лек	пр.	сам.	
1	Свойства информации как объекта защиты	4	1-2	2		2	
2	Актуальность проблемы обеспечения безопасности информации	4	3-4	2		4	опрос
3	Угрозы информационной безопасности. Виды противников и каналы утечки информации.	4	5-6	2	4	4	опрос
4	Вредоносное ПО. Компьютерные вирусы и средства защиты от них	4	7-8	2	4	6	тест
5	Управление рисками	4	9-12	2	2	4	опрос
6	Программно-технические методы защиты	4	13-16	4	4	8	опрос
7	Информационные войны и информационное оружие	4	17-18	4	4	8	тест
	ИТОГО			**18**	**18**	**36**	**зачет**

6. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1 Лекции

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
1	2	3
1	Свойства информации как объекта защиты	Понятие информации. Способы защиты человека от назойливой, недобросовестной информации. Тайна. Виды тайны. Государственная тайна. Опасная информация в формах угроз, клеветы, оскорбления.

1	2	3
2	Актуальность проблемы обеспечения безопасности информации	Основные понятия ИБ: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации. Угрозы ИБ: классификация, источники возникновения и пути реализации. Определение требований к уровню обеспечения ИБ.
3	Угрозы информационной безопасности. Виды противников и каналы утечки информации.	Понятие угрозы. Виды противников или "нарушителей". Окно опасности. Классификация видов угроз ИБ по различным признакам. Угрозы доступности, целостности и конфиденциальности.
4	Вредоносное ПО. Компьютерные вирусы и средства защиты от них	Компьютерный вирус: понятие, пути распространения, проявление действия вируса. Структура современных вирусов: модели поведения вирусов; деструктивные действия вируса; разрушение программы защиты, схем контроля или изменение состояния программной среды; воздействия на программно-аппаратные средства защиты информации. Взлом парольной защиты. Защита от воздействия вирусов. Программы–детекторы, программы–доктора, программы–ревизоры, программы–фильтры.
5	Управление рисками	Основные понятия. Подготовительные этапы управления рисками. Основные этапы управления рисками.
6	Программно-технические методы защиты	Основные понятия программно-технического уровня ИБ. Архитектурная безопасность. Парольная аутентификация. Одноразовые пароли. Идентификация/аутентификация с помощью биометрических данных. Активный аудит. Функциональные компоненты и архитектура. Криптография. Стеганография.
7	Информационные войны и информационное оружие	Определение информационных войн (ИВ). Отличие в целях, характере и способах ведения обычных и ИВ. Противоборствующие стороны в ИВ. Виды информационно-психологического оружия. Роль средств массовой информации в ведении ИВ. Виды манипуляции массовым сознанием. Виды информационно-энергетического воздействия. Психотропные препараты.

6.2. Практические занятия.

Практическое занятие 1. Оценочный расчет защищенности помещений от утечки речевых сообщений по акустическому каналу.

Практическое занятие 2. Оценочный расчет защищенности помещений от утечки информации по электромагнитному каналу.

Практическое занятие 3. Изучение традиционных симметричных криптосистем. Шифры перестановок.

Практическое занятие 4. Изучение традиционных симметричных криптосистем Шифры замены.

Практическое занятие 5. Количественная оценка стойкости парольной защиты

7. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	№ раздела (темы) дисциплины	Форма (вид) самостоятельной работы	Трудоёмкость в академических часах
1	2	3	4
1	Свойства информации как объекта защиты	Работа с лекционным материалом	2
2	Актуальность проблемы обеспечения безопасности информации	Подготовка к практическим занятиям, подготовка к опросу	4

1	2	3	4
3	Угрозы информационной безопасности. Виды противников и каналы утечки информации.	Работа с лекционным материалом. Подготовка к практическим занятиям	4
4	Вредоносное ПО. Компьютерные вирусы и средства защиты от них	Работа с лекционным материалом. Подготовка к опросу	6
5	Управление рисками	Подготовка к практическим занятиям, подготовка к тесту	4
6	Программно-технические методы защиты	Работа с лекционным материалом Подготовка к практическим занятиям	8
7	Информационные войны и информационное оружие	Работа с лекционным материалом. Подготовка к опросу	8
	ИТОГО		**36**

Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине:

Самохвалова С.Г. Информационная безопасность: сборник учебно-методических материалов для направления подготовки 09.03.02. – Благовещенск: Амурский гос. ун-т, 2018. – 65 с. Режим доступа:http://irbis.amursu.ru/DigitalLibrary/AmurSU_Edition/10326.pdf

Внеаудиторная работа студентов представлена: самостоятельным изучением материала теоретических занятий; подготовкой к практическим занятиям; подготовкой к тестам.

Основной целью самостоятельной работы является расширенное и углубленное изучение вопросов, рассматриваемых на лекциях, а также выходящих за рамки аудиторного обучения, но входящего в общий объем знаний дисциплины.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе подготовки по дисциплине используется совокупность методов и средств обучения, позволяющих осуществлять целенаправленное методическое руководство учебно-познавательной деятельностью магистрантов, в том числе на основе интеграции информационных и традиционных педагогических технологий.

При реализации настоящей рабочей программы предусматриваются интерактивные и активные формы проведения занятий, дискуссии по темам исследования и поставленным научным проблемам

Методы и формы организации обучения

ФОО / Методы	Лекция	Пр. зан./	СРС
IT-методы	+	+	+
Работа в команде	+	+	
Лекция-визуализация	+		
Методы проблемного обучения.	+		
Обучение на основе опыта	+		
Опережающая самостоятельная работа			+
Поисковый метод			+
Другие методы	+	+	+

Объем занятий, проводимых в интерактивных формах, составляет 8 академических часов аудиторных занятий.

Тема	Вид занятия	Кол-во академических часов
Вредоносное ПО. Компьютерные вирусы и средства защиты от них	Проблемная лекция	2
Управление рисками	Работа в команде	2
Программно-технические методы защиты	Метод проектов	4
		8

Рекомендуется использование информационных технологий при организации коммуникации со студентами для представления информации, выдачи рекомендаций и консультирования по оперативным вопросам (электронная почта), использование мультимедиа-средств при проведении лекционных и лабораторных занятий.

9. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания, типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций, а так же методические материалы, определяющие процедуры оценивания знаний, умений и навыков отражаются в фонде оценочных средств по дисциплине «Информационная безопасность».

Промежуточная аттестация по итогам освоения дисциплины: зачет.

Вопросы к зачету

1. Проблема «Информационной безопасности».
2. Перечислите составляющие информационной безопасности и их определение.
3. Назовите взаимосвязь между составляющими информационной безопасности. Приведите собственные примеры.
4. Перечислите уровни формирования режима ИБ.
5. Правовые основы ИБ общества.
6. Ответственность за нарушения в сфере ИБ.
7. Перечислите основные механизмы безопасности.
8. Перечислите классы угроз ИБ.
9. Назовите причины и источники случайных воздействий на информационные системы.
10. Перечислите каналы несанкционированного доступа.
11. Что понимается под техническим каналом утечки информации.
12. Охарактеризуйте угрозы доступности информации.
13. Основные угрозы целостности информации.
14. Компьютерные вирусы и ИБ.
15. Назовите классификационные признаки и характерные черты компьютерных вирусов.
16. Назовите вид вирусов, который наиболее распространен в распределенных вычислительных сетях. Почему?
17. Перечислите виды «вирусоподобных» программ.
18. Перечислите виды антивирусных программ.
19. Охарактеризуйте антивирусные сканеры.
20. Назовите факторы, которые определяют качество антивирусных программ.
21. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
22. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
23. Требования к криптосистемам.
24. Основные алгоритмы шифрования.
25. Понятие стеганографии.
26. Уровни ИБ. Основные задачи и положения, решаемые на каждом уровне.
27. Российское и международное законодательство в области защиты информации.
28. Стандарты и спецификации в области защиты информации, их основные положения и принципы построения.
29. Основные механизмы и сервисы безопасности.
30. Административный уровень ИБ (основные понятия, политика безопасности).
31. Управление рисками. Основные понятия, принципы, этапы.
32. Процедурный уровень ИБ, классификация мер этого уровня.
33. Принципы физической и архитектурной безопасности ИС.
34. Идентификация и аутентификация.

10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

а) основная литература

1. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ В.А. Галатенко— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: http://www.iprbookshop.ru/52209.html.— ЭБС «IPRbooks»

2. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ В.Ф. Шаньгин— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: http://www.iprbookshop.ru/63594.html.— ЭБС «IPRbooks»

б) дополнительная литература

1. Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html

2. Смышляев А.Г. Информационная безопасность. Лабораторный практикум [Электронный ресурс] : учебное пособие / А.Г. Смышляев. — Электрон. текстовые данные. — Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2015. — 102 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66655.html

3. Артемов А.В. Информационная безопасность [Электронный ресурс] : курс лекций / А.В. Артемов. — Электрон. текстовые данные. — Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/33430.html

4. Нестеров С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Нестеров С.А.. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с. — 978-5-7422-4331-1. — Режим доступа: http://www.iprbookshop.ru/43960.html

5. Крылов Г.О. Понятийный аппарат информационной безопасности [Электронный ресурс]: словарь/ Г.О. Крылов, С.Л. Ларионова, В.Л. Никитина— Электрон. текстовые данные.— Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016.— 343 с.— Режим доступа: http://www.iprbookshop.ru/64306.html.— ЭБС «IPRbooks»

6. Фомин Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс] : учебно-методическое пособие / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 218 с. — 978-5-4487-0297-6. — Режим доступа: http://www.iprbookshop.ru/77317.html

г) **программное обеспечение и Интернет-ресурсы**

№	Наименование ресурса	Краткая характеристика
1	2	3
1	http://www.iprbookshop.ru/	Электронно-библиотечная система IPRbooks – научно-образовательный ресурс для решения задач обучения в России и за рубежом. Уникальная платформа ЭБС IPRbooks объединяет новейшие информационные технологии и учебную лицензионную литературу. Контент ЭБС IPRbooks отвечает требованиям стандартов высшей школы, СПО, дополнительного и дистанционного образования. ЭБС IPRbooks в полном объеме соответствует требованиям законодательства РФ в сфере образования
2	http://www.e.lanbook.com	Электронная библиотечная система «Издательства Лань», тематические пакеты: математика, физика, инженерно-технические науки, химия
3	http://www.itsec.ru	Электронный журнал по информационной безопасности.

1	2	3
4	http://elibrary.ru	Научная электронная библиотека журналов
5	MS Windows 7 Pro	Операционная система MS Windows 7 Pro - DreamSpark Premium Electronic Software Delivery (3 years) Renewal по договору - Сублицензионный договор № Tr000074357/KHB 17 от 01 марта 2016 года
6	LibreOffice	Пакет прикладных программ, бесплатное распространение по лицензии MozillaPublicLicenseVersion 2.0 http://www.libreoffice.org/download/license/
7	7-Zip	Программа-архиватор, бесплатное распространение по лицензии GNU LGPL http://www.7-zip.org/license.txt

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для обеспечения систематической и регулярной работы по изучению дисциплины и успешного прохождения текущей и промежуточной аттестации студенту рекомендуется придерживаться следующего порядка обучения:

1. Самостоятельно определить объем времени, необходимого для проработки каждой темы.

2. Регулярно изучать каждую тему дисциплины, используя различные формы индивидуальной работы.

При подготовке к практическим занятиям обязательно требуется изучение дополнительной литературы по теме занятия.

Самостоятельная работа по дисциплине «Информационная безопасность» включает: работу с первоисточниками; подготовку к практическим занятиям и тестам; подготовку к текущей и промежуточной аттестации по дисциплине.

Для теоретического и практического усвоения дисциплины большое значение имеет самостоятельная работа студентов, которая может осуществляться студентами индивидуально и под руководством преподавателя.

Самостоятельная работа студентов предполагает самостоятельное изучение отдельных тем, дополнительную подготовку студентов к каждому лабораторному занятию.

В процессе изучения дисциплины «Информационная безопасность» обучающиеся должны выполнить следующие виды самостоятельной работы: самоподготовку к учебным занятиям по конспектам, учебной литературе и с помощью электронных ресурсов; подготовка к тестированию по темам дисциплины.

Формой самостоятельной работы является работа с литературой. Овладение методическими приемами работы с литературой - одна из важнейших задач студента. Работа с литературой включает следующие этапы: предварительное знакомство с содержанием; углубленное изучение текста с преследованием следующих целей: усвоить основные положения; усвоить фактический материал; логическое обоснование главной мысли и выводов.

При подготовке к промежуточной аттестации целесообразно: внимательно изучить перечень вопросов и определить, в каких источниках находятся сведения, необходимые для ответа на них; внимательно прочитать рекомендованную литературу; составить краткие конспекты ответов (планы ответов).

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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

Лекции проводятся в лекционной аудитории, оборудованной проектором, экраном, учебной доской, ноутбуком.