Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.14 Кибербезопасность

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

09.03.03 Прикладная информатика

Направленность (профиль)

09.03.03.33 Прикладная информатика: цифровая экономика

Форма обучения очная

Год набора 2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили

Доцент, Юронен Е.А.

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Цель преподавания дисциплины: подготовка будущих специалистов-практиков к использованию современных методов и средств защиты информации в организационно-управленческой и аналитической деятельности.

1.2 Задачи изучения дисциплины

- формирование знаний о концепциях защиты информации и системах безопасности персональных компьютеров и компьютерных сетей;

-изучить теорию и практику новейших достижений и перспектив в развития в области создания систем безопасности локальных вычислительных сетей и сети Internet;

- формирование знаний о криптографических методах зашиты информации; основах криптографии; основных методах и приемах защиты от несанкционированного доступа; о компьютерных вирусах и антивирусных программах; организационно-правовом

обеспечение ИБ;

- развитие способности работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;

- овладение способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;

- формирование навыков выбора инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации и умения обосновывать свой выбор.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине
ПК-4: Способен проводить предпроектное обследование организации и выявлять требования к ИС	
ПК-4.1: Знает: инструменты и методы выявления требований; возможности типовой ИС; современные стандарты информационного взаимодействия систем	- содержание базовых определений и понятий, проблемы информационной безопасности; содержание структур, назначений, особенностей и краткой характеристики функциональных возможностей различных технологий информационной безопасности, организационно-технических, законодательных, программно-аппаратных, математических и т.п. средств их реализации

	- ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития - навыками работы с различными информационными ресурсами и технологиями
ПК-4.2: Умеет: анализировать исходную документацию; проводить интервью	- современное состояние и развитие методов и средств информационной безопасности, методику их применения для решения задач практических задач различного уровня - выявлять угрозы информационной безопасности на основе инструментальной обработки информации - навыками проведения интервью и анализа документации
ПК-4.3: Владеет навыками: сбора данных о запросах и потребностях заказчика применительно к типовой ИС; документировать собранные данные в соответствии с регламентами организации	- состав и функциональные возможности инструментальных средств и информационных технологий обработки информации для решения профессиональных задач кибербезопасности - обосновывать выбор средств для решения конкретных задач информационной безопасности; сводить постановки задач на содержательном уровне к формальным и относить их к соответствующим информационным технологиям - навыками анализа информационной инфраструктуры государства и общества и навыками работы с прикладными технологиями, используемыми при проектировании и эксплуатации систем информационной безопасности различных уровней

1.4 Особенности реализации дисциплины

Язык реализации дисциплины: Русский.

Дисциплина (модуль) реализуется без применения ЭО и ДОТ.

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	е 1
Контактная работа с преподавателем:	**1,5 (54)**	
занятия лекционного типа	0,5 (18)	
практические занятия	1 (36)	
Самостоятельная работа обучающихся:	**1,5 (54)**	
курсовое проектирование (КП)	Нет	
курсовая работа (КР)	Нет	

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Модули, темы (разделы) дисциплины	Контактная работа, ак. час.							
		Занятия лекционного типа		Занятия семинарского типа				Самостоятельная работа, ак. час.	
				Семинары и/или Практические занятия		Лабораторные работы и/или Практикумы			
		Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС
1. Введение									
	1. Основные термины и понятия. Угрозы кибербезопасности.	2							
	2. Угрозы кибербезопасности.	2							
	3. Уровни и стандарты информационной безопасности.	2							
	4. Разработка требований к системе и структуры системы кибербезопасности			6					
	5. Анализ рисков безопасности разработанной системы			6					
	6. Разработка документации для системы безопасности			6					
	7. Изучение теоретического материала							6	
	8. Подготовка и выполнение практических работ							12	
	9. Подготовка и защита реферата							6	
2. Безопасность информационных систем									
	1. Вредоносное программное обеспечение и защита от него.	2							

2. Обеспечение доступности и защищенности информационных систем.	4							
3. Разработка программы криптозащиты канала связи			6					
4. Разработка программы криптозащиты данных, хранящихся на носителе			6					
5. Изучение теоретического материала							6	
6. Подготовка и выполнение практических работ							10	
3. Киберпреступность и способы ее предотвращения								
1. Проект модели угроз кибербезопасности.	6							
2. Разработка должностных инструкций по внедрению и эксплуатации ПО, обеспечивающего кибербезопасность			6					
3. Изучение теоретического материала							6	
4. Подготовка и выполнение практических работ							8	
Всего	18		36				54	

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Зыкова Т. В., Сидорова Т. В., Шершнева В. А. Основы информационной безопасности: учебное пособие для студентов вузов по направлению подготовки бакалавров 230700.62 "Прикладная информатика" и 080500.62 "Бизнес-информатика"(Красноярск: СФУ).
2. Бухтояров М. С., Бухтоярова А. А., Козлова М. В., Елизова Л. А. Гуманитарные, социальные и философские аспекты информационной безопасности: учебно-методическое пособие(Красноярск: СФУ).
3. Рогалев А. Н. Математическое моделирование в задачах информационной безопасности: учеб. пособие(Красноярск: ИПЦ КГТУ).
4. Емельянов С. В. Труды Института системного анализа Российской академии наук : Т. 61. Управление кибербезопасностью больших систем. Системные проблемы кибербезопасности. Технологии кибербезопасности(Москва: URSS).
5. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства: учеб. пособие для студентов вузов(Москва: ДМК Пресс).

4.2 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства (программное обеспечение, на которое университет имеет лицензию, а также свободно распространяемое программное обеспечение):

1. □ электронные таблицы Excel;
2. □ средство для создания и просмотра презентаций “Microsoft Office PowerPoint”.

4.3 Интернет-ресурсы, включая профессиональные базы данных и информационные справочные системы:

1. Каждый обучающийся в течение всего периода обучения по дисциплине обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам (электронным библиотекам) и к электронной информационно-образовательной среде Университета. Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают возможность доступа обучающегося из любой точки, в которой имеется доступ к сети Интернет, и отвечают техническим требованиям организации, как на территории Университета, так и вне ее.
2. Электронная информационно-образовательная среда Университета обеспечивает:
3. □ доступ к учебным планам, рабочим программам дисциплин (модулей), практик, и к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочих программах;

4. фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения основной образовательной программы;

5. проведение всех видов занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

6. формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы со стороны любых участников образовательного процесса;

7. взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети Интернет.

8.

5 Фонд оценочных средств

Оценочные средства находятся в приложении к рабочим программам дисциплин.

6 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе:

- ПЭВМ с доступом в Интернет (операционная система, офисные программы, антивирусные программы);
- мультимедийный проектор с дистанционным управлением.