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 2020

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;
- изучение теории и практики 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	основные стандарты в области информационных систем выявлять информационные потребности способами автоматизации документооборота на различных этапах жизненного цикла информационных систем

ПК-4.2: Умеет: анализировать исходную документацию; проводить интервью	методы анализа прикладной области, информационных потребностей проводить анализ предметной области методами выполнения технико-экономического
	обоснования проектных решений
ПК-4.3: Владеет навыками: сбора данных о запросах и потребностях заказчика применительно к типовой ИС; документировать собранные данные в соответствии с регламентами организации	содержание стадий и этапов канонического и типового проектирования разрабатывать требования к информационным системам навыками анализа рынка программно-технических средств, ИКТ для создания и модификации информационных систем
УК-10: Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	
УК-10.1: Понимает негативные последствия коррупции как угрозы национальной безопасности государства, а также основные принципы противодействия коррупции в Российской Федерации	основные принципы противодействия коррупции в РФ прогнозировать негативные последствия коррупции основами антикоррупционной деятельности
УК-10.2: Демонстрирует нетерпимое отношение к коррупции,реализует меры антикоррупционной профилактики в повседневной жизни и профессиональной деятельности	негативное влияние коррупции в профессиональной деятельности и повседневной жизни использовать меры антикоррупционной профилактики в повседневной жизни мерами антикоррупционной профилактики в профессиональной деятельности

1.4 Особенности реализации дисциплины

Язык реализации дисциплины: Русский.

Дисциплина (модуль) реализуется с применением ЭО и ДОТ

URL-адрес и название электронного обучающего курса: https://e.sfu-kras.ru/course/view.php?id=30964.

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. Основные термины, понятия и категории знаний информационной безопасности									
	1. Информационная безопасность: общие сведения и понятия	3							
	2. Угрозы кибербезопасности	3							
	3. Анализ современных понятий информационной безопасности			4					
	4. Глоссарий. Терминология в сфере кибербезопасности			4					
	5. Защита персональных данных			4					
	6. Изучение теоретического материала							4	
	7. Подготовка и выполнение практических работ							14	
	8. Подготовка и защита реферата							6	
2. Нормативно-правовое регулирование процессов информационной безопасности и защиты данных									
	1. Государственное регулирование информационной безопасности	3							
	2. Стандарты информационной безопасности	3							

3. Работа с ГОСТами в области информационной безопасности			4					
4. Оценка информационных угроз и рисков организации			4					
5. Изучение теоретического материала							4	
6. Подготовка и выполнение практических работ							10	
3. Механизмы и инструменты защиты данных в АИС организации								
1. Механизмы обеспечения информационной безопасности	2							
2. Организация системы защиты АИС	2							
3. Модели информационной безопасности	2							
4. Программные средства защиты данных			4					
5. Криптографические средства защиты информации			6					
6. Анализ системы информационной безопасности для организаций			6					
7. Изучение теоретического материала							4	
8. Подготовка и выполнение практических работ							12	
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.