Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-ВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ М.К. АММОСОВА»
Финансово-экономический институт

Рабочая программа дисциплины

Б1.В.ДВ.1.2 Информационная безопасность

для программы бакалавриата
по направлению подготовки 38.03.01 Экономика
направленность (профиль): Общий
Форма обучения: заочная

Автор(ы): Панова Ия Иннокентьевна, старший преподаватель, кафедра «Математическая экономика и прикладная информатика», ii.panova@s-vfu.ru

РЕКОМЕНДОВАНО Заведующий кафедрой разработчика _____ _____/_____ протокол №_____ от «___»_____20__ г.	ОДОБРЕНО Заведующий выпускающей кафедрой «Экономика и финансы» _____/Г.И. Рац протокол № 24 от « 11 » апреля 2019 г.	ПРОВЕРЕНО Нормоконтроль в составе ОП пройден Специалист УМО/деканата _____ /А.И. Сергеева « 22 » апреля 2019 г.
Рекомендовано к утверждению в составе ОП Председатель УМК _____/ А.П. Соловьева протокол УМК № 6 от « 24 » апреля 2019 г.		Эксперт УМК _____ / Л.Н. Попова « 19 » апреля 2019 г.

Якутск 2019

1. АННОТАЦИЯ
к рабочей программе дисциплины
Б1.В.ДВ1.2 Информационная безопасность

Трудоемкость 2 з.е.

1.1. Цель освоения и краткое содержание дисциплины

Цель освоения: обеспечить будущих бакалавров теоретическими знаниями и практическими навыками в области защиты информации и информационной безопасности, необходимыми при выполнении профессиональных задач с использованием информационно-телекоммуникационных технологий.

Краткое содержание дисциплины: Основы информационной безопасности. Методы и средства обеспечения информационной безопасности.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения программы (содержание и коды компетенций)	Планируемые результаты обучения по дисциплине
ОПК-1 Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (в т.ч. работать с информацией в глобальных компьютерных сетях) ПК-8 Способность использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии	Знать • Основные понятия и определения ИБ. • Основы криптографии • Основные методы и приемы защиты от несанкционированного доступа • Вредоносные программы и антивирусные программы Уметь • применять программное обеспечение для защиты от несанкционированного доступа; • применять программное обеспечение для защиты от вирусного заражения компьютера; • зашифровывать и дешифровывать сообщения различными методами; Владеть (методиками) • построения неформальной модели нарушителя Владеть практическими навыками • работы с программными и техническими средствами защиты информации.

1.3. Место дисциплины в структуре образовательной программы

Индекс	Наименование дисциплины (модуля), практики	Семестр изучения	Индексы и наименования учебных дисциплин (модулей), практик	
			на которые опирается содержание данной дисциплины (модуля)	для которых содержание данной дисциплины (модуля) выступает опорой
Б1.В.ДВ.1.2	Информационная безопасность	1	-	Б3 Итоговая государственная аттестация

1.4. Язык преподавания: русский

2. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Выписка из учебного плана:

Код и название дисциплины по учебному плану	Б1.В.ДВ.1.2 Информационная безопасность	
Курс изучения	1	
Семестр(ы) изучения	1	
Форма промежуточной аттестации (зачет/экзамен)	зачет	
Курсовой проект/ курсовая работа (указать вид работы при наличии в учебном плане), семестр выполнения	не предусмотрено	
Трудоемкость (в ЗЕТ)	2	
Трудоемкость (в часах) (сумма строк №1,2,3), в т.ч.:	72	
№1. Контактная работа обучающихся с преподавателем (КР), в часах:	Объем аудиторной работы, в часах	В т.ч. с применением ДОТ или ЭО, в часах
Объем работы (в часах) (1.1.+1.2.+1.3.):	13	
1.1. Занятия лекционного типа (лекции)	4	
1.2. Занятия семинарского типа, всего, в т.ч.:	6	
- семинары (практические занятия, коллоквиумы и т.п.)	6	
- лабораторные работы		
- практикумы		
1.3. КСР (контроль самостоятельной работы, консультации)	2	
№2. Самостоятельная работа обучающихся (СРС) (в часах)	55	
№3. Количество часов на экзамен (зачет)	4	

3. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий

3.1. Распределение часов по темам и видам учебных занятий

Тема	Всего часов	Контактная работа, в часах									Часы СРС
		Лекции	из них с применением ЭО и ДОТ	Семинары (практические занятия, коллоквиумы)	из них с применением ЭО и ДОТ	Лабораторные работы	из них с применением ЭО и ДОТ	Практикумы	из них с применением ЭО и ДОТ	КСР (консультации)	
Тема 1. Основы информационной безопасности.	25	2		2						1	20
Тема 2. Методы и средства зашиты информации.	43	2		4						2	35
Всего часов	68	4		6						3	55

3.2. Содержание тем программы дисциплины

Тема 1. Основы информационной безопасности.
Компоненты модели информационной безопасности. Неформальная модель нарушителя. Обеспечение защиты информации. Правовое обеспечение информационной безопасности. Виды защищаемой информации. Нормы уголовного кодекса, предусматривающие ответственность за совершение преступлений в сфере компьютерной информации.

Тема 2. Методы и средства защиты информации.
Аппаратно-технические и программные средства защиты информации. Криптографические методы защиты информации. Электронно-цифровая подпись. Вредоносные программы и антивирусное программное обеспечение.

3.3. Формы и методы проведения занятий, применяемые учебные технологии

При проведении занятий и организации СРС используются традиционные технологии сообщающего обучения, предполагающие передачу информации в готовом виде: проведение лекционных занятий, самостоятельная работа с источниками. Предусмотрено использование активных и интерактивных форм обучения с целью формирования и развития профессиональных навыков студентов - выполнение практических работ с применением компьютерных технологий.

4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

4.1. Содержание СРС

№	Наименование раздела (темы) дисциплины	Вид СРС	Трудо-емкость (в часах)	Формы и методы контроля
1	Тема 1. Основы информационной безопасности.	Проработка теоретического материала. Выполнение практических работ	20	Устный опрос, проверка конспектов Проверка практических работ
2	Тема 2. Методы и средства защиты информации.	Проработка теоретического материала. Выполнение практических работ	35	Устный опрос, проверка конспектов Проверка практических работ

4.2. Перечень практических работ

Практическая работа №1
«Модель нарушителя»

Построить модель нарушителя для предприятия/организации некоторой предметной области по выбору. Рекомендации по выбору: предметная область должна быть вам хорошо знакома с точки зрения основных процессов и сопровождающих их информационных потоков.

Практическая работа №2
«Криптографические методы. Симметричные алгоритмы»

В соответствии с изученными криптографическими методами симметричного шифрования выполнить процедуры шифрования и дешифрования сообщений.

Практическая работа №3
«Криптографические методы. Асимметричные алгоритмы»

В соответствии с изученными криптографическими методами асимметричного шифрования выполнить процедуры шифрования и дешифрования сообщений.

Практическая работа №4
«Программные средства защиты. Парольная защита»

Выполнить задания по определению достаточных характеристик (мощности алфавита, длины) пароля, отвечающего предложенным критериям безопасности. Опробовать и проанализировать (сравнить возможности) различных менеджеров паролей.

5. Методические указания для обучающихся по освоению дисциплины

В соответствии с программой дисциплины должны быть изучены следующие разделы:

Тема 1. Основы информационной безопасности.

Тема 2. Методы и средства защиты информации.

Теоретический материал в СДО Moodle изложен в указанном порядке, поскольку каждая последующая тема основана на понимании некоторых сведений из предыдущих.

При изучении каждой темы самостоятельно следует:

- внимательно ознакомиться с теоретическим материалом (прочитать текст лекции);
- выполнить конспектом теоретического материала, ознакомиться при необходимости с дополнительной литературой по данной теме.

В диагностическом разделе дисциплины приведены вопросы и тесты к каждой теме дисциплины, которые необходимо выполнить для закрепления теоретических знаний. Основной самостоятельной работой является подготовка и сбор материала для выполнения практических работ.

Последовательное и добросовестное изучение курса является одной из основ формирования системного подхода к вопросам обеспечения информационной безопасности.

Рейтинговый регламент по дисциплине:

Вид выполняемой учебной работы (контролирующие мероприятия)	Количество баллов (min)	Количество баллов (max)
Посещаемость	5	10
Конспектирование и СРС (6 заданий) Оценивается в 5 баллов Оценивается полнота проведенного исследования, ответа на поставленный вопрос и качество оформления результатов: 2 б - раскрыты основные понятия, определения 2 б – проведен анализ, присутствуют выводы 1 б - оформление результатов работы	20	30
Выполнение практических работ (4 работы) Оценивается в 10 баллов, из них: 4 б - предварительный анализ задачи (сбор и подготовка данных) 4 б – обоснование применяемых методов (на основе материалов лекций и СРС) 2 б - оформление результатов работы	20	40
Контрольная работа	**15**	**20**
Количество баллов для получения зачета (min-max)	**60**	**100**

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1. Показатели, критерии и шкала оценивания

Коды оцениваемых компетенций	Показатель оценивания (дескриптор) (по п.1.2.РПД)	Уровни освоения	Критерий оценивания	Оценка
ОПК-1 ПК-8	Знать • Основные понятия и определения ИБ. • Основы криптографии • Основные методы и приемы защиты от несанкционированного доступа • Вредоносные программы и антивирусные программы	Высокий	Практические работы оценены не менее, чем на 30 баллов. Обучающийся знает: • содержание основных понятий обеспечения информационной безопасности; • основы криптографии • методы и приемы защиты от несанкционированного доступа; • принцип действия и классификацию вредоносных программ Обучающийся умеет:	зачтено

	Уметь • применять программное обеспечение для защиты от несанкционированного доступа; • применять программное обеспечение для защиты от вирусного заражения компьютера; • зашифровывать и дешифровывать сообщения различными методами; Владеть (методиками) • построения неформальной модели нарушителя • практическими навыками работы с программными и техническими средствами защиты информации.		• применять программное обеспечение для защиты от несанкционированного доступа; • применять программное обеспечение для защиты от вирусного заражения компьютера; • зашифровывать и дешифровывать сообщения различными методами; Обучающийся владеет методиками: • построения неформальной модели нарушителя; • практическими навыками работы с программными и техническими средствами защиты информации.	
		Базовый	Практические работы оценены не менее, чем на 25 баллов. Обучающийся знает: • содержание основных понятий обеспечения информационной безопасности; • основы криптографии • методы и приемы защиты от несанкционированного доступа; • классификацию вредоносных программ Обучающийся умеет: • применять программное обеспечение для защиты от несанкционированного доступа; • применять программное обеспечение для защиты от вирусного заражения компьютера; • зашифровывать и дешифровывать сообщения; Обучающийся владеет: • методикой построения неформальной модели нарушителя; • практическими навыками работы с программными средствами защиты информации	зачтено
		Мини-мальный	Практические работы оценены не менее, чем на 20 баллов. Обучающийся знает: • содержание основных понятий обеспечения	зачтено

			информационной безопасности; • классификацию угроз информационной безопасности; • классификацию вредоносных программ Обучающийся умеет: • применять программное обеспечение для защиты от несанкционированного доступа; • применять программное обеспечение для защиты от вирусного заражения компьютера; Обучающийся владеет: • методикой построения неформальной модели нарушителя.	
		Не освоены	Практические работы оценены менее, чем на 20 баллов. Обучающийся не знает: • содержание основных понятий обеспечения информационной безопасности; • классификацию угроз информационной безопасности; • классификацию вредоносных программ Обучающийся не умеет: • применять программное обеспечение для защиты от несанкционированного доступа; • применять программное обеспечение для защиты от вирусного заражения компьютера; Обучающийся не владеет методикой построения неформальной модели нарушителя.	не зачтено

6.2. Типовые контрольные задания (вопросы) для промежуточной аттестации

Коды оцениваемых компетенций	Оцениваемый показатель (ЗУВ)	Тема	Образец типового (тестового или практического) задания (вопроса)
ОПК-1 ПК-8	Знать • Основные понятия и определения ИБ.	Тема 1. Основы информационной безопасности.	*Образец теста:* Что представляет собой доктрина информационной безопасности РФ? 1. Нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;

	• Основы криптографии Уметь • зашифровывать и дешифровывать сообщения различными методами; Владеть (методиками) • построения неформальной модели нарушителя		2. Федеральный закон, регулирующий правоотношения в области информационной безопасности; 3. Целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов; 4. Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. *Образец практического задания:* Используя алгоритм RSA с заданными параметрами сгенерировать открытый и закрытый ключ зашифровать сообщение. *Образец практического задания:* Постройте неформальную модель нарушителя для заданной предметной области.
	Знать • Основные методы и приемы защиты от несанкционированного доступа • Вредоносные программы и антивирусные программы Уметь • применять программное обеспечение для защиты от несанкционированного доступа; • применять программное обеспечение для защиты от вирусного заражения компьютера; Владеть практическими навыками работы с программными и техническими средствами защиты информации.	Тема 2. Методы и средства защиты информации.	*Образец теста:* Какие недостатки имеют системы обнаружения вторжений, работающие на основе обнаружения аномалий? 1. Высокий процент ложных срабатываний; 2. Способны контролировать ситуацию во всей сети; 3. Неспособны анализировать степень проникновения; 4. Работа затруднена при высокой загрузке сети; 5. Снижается эффективность работы сервера, на котором они установлены *Образец практического задания:* Рассчитать минимальный срок действия пароля, при котором обеспечивается требуемый уровень надежности парольной защиты. Исходные данные: Вероятность вскрытия 10-5. Мощность алфавита – 10 знаков. Длина пароля – 6 знаков. Скорость интерактивного подбора паролей – 12 паролей/минуту.

6.3. Методические материалы, определяющие процедуры оценивания

Форма промежуточной аттестации: Зачет

Данный вид комплексного испытания предполагает последовательное выполнение всех форм текущего контроля, таких, как тесты, контрольные работы, расчетно-графические работы.

Проверка выполнения заданий СРС.

Конспект: данная форма контроля позволяет оценить степень усвоения теоретического материала, выделенного на самостоятельное изучение.

Ответы на вопросы: данная форма контроля направлена на оценку степени знания и владения изучаемыми методиками.

Тестирование. Данная форма контроля направлена на оценку:

- Основных теоретических знаний обучающегося по мере освоения основных разделов дисциплины. В ходе теоретического обучения предполагается тест по теме 1.

- Степени владения изучаемыми методологиями и средствами программными и аппаратными. Тест по теме 2.

Практические работы. В этой форме промежуточного контроля проверяются способности решения предметно-ориентированных задач.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

№	Автор, название, место издания, издательство, год издания учебной литературы, вид и характеристика иных информационных ресурсов	Наличие грифа, вид грифа	НБ СВФУ, кафедральная библиотека и кол-во экземпляров	Электронные издания: точка доступа к ресурсу (наименование ЭБС, ЭБ СВФУ)
Основная литература				
1	Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с.			Режим доступа: www.iprbookshop.ru/22424
2	Шаньгин В. Ф., Информационная безопасность и защита информации. [Электронный ресурс]/ Шаньгин В. Ф. — М.: ДМК Пресс, 2014. — 702 .			Режим доступа: www.studentlibrary.ru/book/ISBN9785940747680
Дополнительная литература				
1	Чернова Е. В. Информационная безопасность человека: учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — М.: Юрайт, 2020. — 243 с.			Режим доступа: https://urait.ru/bcode/449350
2	Богатырев В. А. Информационные системы и технологии. Теория надежности: учебное пособие для вузов / В. А. Богатырев. — М.: Юрайт, 2020. — 318 с.			Режим доступа: https://urait.ru/bcode/451108
3	Мельников В. П., Информационная безопасность и защита информации: учебное пособие для студ. высш. учеб. заведений. — М.: Академия, 2008. — 336 с.		НБ СВФУ - 1	

.8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее сеть-Интернет), необходимых для освоения дисциплины

1. http://fstec.ru/ - сайт Федеральной службы по техническому и экспортному контролю

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№	Тип учебного занятия	Аудитория	Перечень оборудования
1	Лекция	677000, Республика Саха (Якутия), г. Якутск, ул. Белинского, д. 58, ауд. 307 НБ	Компьютер персональный, Aguarius Elt (21 шт.); Монитор, Aquarius (22 шт.); Принтер Xerox (1 шт.); Интерактивная система тип 1: Интерактивная доска ActivBoard PRM-AB378-03, DLP Проектор торговой марки PROMETHEAN модели PRM-35, Крепление для проектора настенное торговой марки Promethean, модель Mount DLP (1 комплект); Доска аудиторная, 3-х створчатая (1 шт.); Стол аудиторный (16 шт.); Стол компьютерный (23 шт.); Стул (55 шт.).
2	Практическое занятие	677000, Республика Саха (Якутия), г. Якутск, ул. Белинского, д. 58, ауд. 307 НБ	Компьютер персональный, Aguarius Elt (21 шт.); Монитор, Aquarius (22 шт.); Принтер Xerox (1 шт.); Интерактивная система тип 1: Интерактивная доска ActivBoard PRM-AB378-03, DLP Проектор торговой марки PROMETHEAN модели PRM-35, Крепление для проектора настенное торговой марки Promethean, модель Mount DLP (1 комплект); Доска аудиторная, 3-х створчатая (1 шт.); Стол аудиторный (16 шт.); Стол компьютерный (23 шт.); Стул (55 шт.).
3	Самостоятельная работа студентов (СРС)	677000, Республика Саха (Якутия), г. Якутск, ул. Белинского, д. 58, НБ СВФУ, 204, 210, 212	ПК, терминальные станции, учебные комплекты (столы и стулья)

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

10.1. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии:

- использование на занятиях электронных изданий (чтение лекций с использованием слайд-презентаций, электронного учебного пособия);
- использование специализированных и офисных программ, информационных (справочных) систем;

• организация взаимодействия с обучающимися посредством электронной почты и СДО Moodle.

10.2. Перечень программного обеспечения

Лицензионное программное обеспечение

- Dr.Web Enterprise Security Suite: Dr.Web Desktop Security Suite (Комплексная защита); Dr.Web Server Security Suite (Антивирус); Медиапакет Dr.Web сертифицированный ФСТЭК России,
- Microsoft Windows 10 Корпоративная ,
- Microsoft Office,
- сервис ZOOM, тариф Образование.

Открытое программное обеспечение

- OpenOffice,
- LibreOffice

10.3. Перечень информационных справочных систем

1) http://www.consultant.ru – Справочно-правовая система Консультант+. Содержит законодательную базу, нормативно - правовое обеспечение, статьи.
2) http://www.garant.ru – Информационно-правовой портал Гарант. Содержит законодательную базу, нормативно - правовое обеспечение, статьи.

ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Б1.В.ДВ1.2 Информационная безопасность

Учебный год	Внесенные изменения	Преподаватель (ФИО)	Протокол заседания выпускающей кафедры (дата, номер), ФИО зав.кафедрой, подпись
2020-2021	Внесены изменения в п.7 в связи с истечением срока доступа к источникам в ЭБС	Панова И.И.	Протокол №59 от 24.09.2020 г. Рац Г.И.