МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Костромской государственный университет»

(КГУ)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки 38.03.01 «Экономика»

Направленность «Учет и анализ бизнес-процессов»

Квалификация выпускника: бакалавр

Кострома

2020

Рабочая программа дисциплины «Информационная безопасность» разработана:

- в соответствии с Федеральным государственным образовательным стандартом по направлению подготовки 38.03.01 «Экономика» (уровень бакалавриата), утвержденным приказом Минобрнауки РФ № 1327 от 12.11.2015

- в соответствии с учебным планом направления подготовки 38.03.01«Экономика» (уровень бакалавриата), направленность «Учет и анализ бизнес-процессов», год начала подготовки 2020 (очная форма обучения).

Разработал: Виноградова Г.Л., к.т.н, доцент кафедры защиты информации

Рецензент: Волков А.А., к.т.н., доцент кафедры защиты информации

УТВЕРЖДЕНО:
На заседании кафедры бухгалтерского учета и аудита
Протокол заседания кафедры № 9 от _07.05.2020_ г.

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА
На заседании кафедры бухгалтерского учета и аудита
Протокол заседания кафедры № 9 от _13.05.2021_ г.

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА
На заседании кафедры бухгалтерского учета и аудита
Протокол заседания кафедры № 7 от _16.03.22_ г.
.

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА
На заседании кафедры бухгалтерского учета и аудита
Протокол заседания кафедры № 9 от _17.05.2023_ г.

1. Цели и задачи освоения дисциплины

Цель дисциплины: формирование знаний о сущности информационной безопасности, ее роли в системе управления организацией, сущности и характере угроз в информационной сфере, а также формирование умений и навыков по реализации, способов и средств защиты информации.

В результате изучения учебной дисциплины «Информационная безопасность» у обучаемых должны сформироваться профессиональные компетенции:

- способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1);

Задачи дисциплины:

- изучение основных понятий в области защиты информации, основных видов информации ограниченного доступа, принципов обеспечения безопасности информации в организации финансово-кредитной сферы;
- изучение актуальных угроз безопасности информации, характерных для обработки в информационных системах организаций и способов и средств защиты информации;
- формирование умений анализа актуальных угроз безопасности, их классификации и оценки с точки зрения возможного ущерба для деятельности организации;
- формирование умений осуществления выбора правовых, организационных и технических средств защиты информации для выполнения требований по обеспечению безопасности информации;
- приобретение навыков разработки нормативно-правовых документов, с учетом выполнения требований политики информационной безопасности организации.

2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

знать

– основные понятия в области защиты информации;

- основные виды информации ограниченного доступа;
- принципы обеспечения безопасности информации в организации финансово-кредитной сферы, в том числе сведений составляющих государственную тайну;
- актуальные угрозы безопасности информации организации с учетом ее специфики;
- современные способы и средства защиты информации;

уметь

- разрабатывать перечень информации ограниченного доступа в соответствии с особенностями деятельности организации;
- анализировать и классифицировать актуальные угрозы безопасности информации и оценивать их с точки зрения возможного ущерба для деятельности организации;

- осуществлять выбор правовых, организационных и технических средств защиты информации для выполнения требований по обеспечению безопасности информации;

владеть

- навыками разработки нормативно-правовых документов, с учетом выполнения требований политики информационной безопасности организации;

- навыками оценки угроз информационной безопасности для объекта информатизации организаций финансово-кредитной сферы.

освоить компетенции:

- способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1);

3. Место дисциплины в структуре ОП ВО

Дисциплина «Информационная безопасность» относится блоку Б1.Б.17 к обязательной дисциплине базовой части учебного плана, при этом, в значительной степени отличается от других дисциплин сферой знаний и направленностью обучения. Именно эта дисциплина формирует у обучаемых способность применения знаний и практических навыков в области защиты информации с целью обеспечения защиты от угроз информационных активов экономической деятельности.

Дисциплина изучается на первом курсе, требования к входным знаниям, умениям и навыкам определяются требованиями к уровню подготовки по дисциплине «Информатика» за курс средней школы.

Изучение дисциплины является основой для освоения последующих дисциплин/практик: «Теория организации и управления», «Документационное обеспечение деятельности организации», «Профессиональные компьютерные программы».

Знания, умения и навыки, полученные в ходе освоения дисциплины безусловно будут использованы в дальнейшем в профессиональной деятельности.

Освоение данной дисциплины необходимо как предшествующее для прохождения производственной (преддипломной) практики, написания выпускной квалификационной работы.

Формирование профессиональных компетенций ОПК-1 происходит также на других профильных дисциплинах, раскрывая единство и взаимосвязь профильных дисциплин.

Дисциплина относится блоку Б.1.Б.17 к дисциплинам базовой части учебного плана. Изучается в 2 семестре обучения (очная форма), 4, 5 семестрах (заочная форма и заочная форма по индивидуальному плану)

Изучение дисциплины основывается на ранее освоенных дисциплинах:

Микроэкономика; макроэкономика; финансы; мировая экономика и международные экономические отношения; финансовое право; корпоративное право, бухгалтерский учет и анализ.

Изучение дисциплины является основой для освоения последующих дисциплин:

банковское дело; финансовые рынки; анализ деятельности коммерческого банка; банковский менеджмент; национальная платежная система; учет и операционная деятельность в банках, учебные и производственные практики

4. Объем дисциплины (модуля)

4.1. Объем дисциплины в зачетных единицах с указанием академических (астрономических) часов и виды учебной работы

Виды учебной работы,	Очная форма
Общая трудоемкость в зачетных единицах	3
Общая трудоемкость в часах	108
Аудиторные занятия в часах, в том числе:	32
Лекции	16
Практические занятия	16
Лабораторные занятия	
ИКР	0,25
Самостоятельная работа в часах, в том числе:	75,75
Форма промежуточной аттестации	зачет

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	32
Практические занятия	32
Лабораторные занятий	-
Консультации	
Зачет/зачеты	0,25
Курсовые работы	-
Курсовые проекты	-
Всего	32,25

5.Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием количества часов и видов занятий

Очная форма обучения

№	Название раздела, темы	Всего час	Аудиторные занятия			Самостоятельная работа
			Лекц.	Практ.	Лаб.	
1	Виды информации ограниченного доступа, понятие тайны.	14	2	2		10
2	Классификация угроз безопасности информации	14	2	2		10
3	Правовая защита информации	14	2	2		10
4	Организация защиты информации	14	2	2		10
5	Физическая и программно-техническая защи-	12	2	2		10

	та информации					
6	Криптографическая защита информации.	14	2	2		10
7	Требования по обеспечению информационной безопасности	22,75	4	4		15,75
	зачет	4				4+0,25
	Итого:	108	16	16		76

5.2. Содержание:

ТЕМА 1.. Виды информации ограниченного доступа, понятие тайны.
Основные понятия дисциплины «Информационная безопасность». Законодательство ИБ. Виды информации ограниченного доступа: государственная тайна, конфиденциальная информация. Виды тайн (коммерческая, банковская, служебная, кредитной истории, тайна страхования, налоговая тайна, аудиторская тайна. Информация, к которой нельзя ограничивать доступ.

ТЕМА 2.. Классификация угроз безопасности информации.
Понятие угрозы информационной безопасности. Источники угроз. Классификации угроз ИБ. Методы оценки опасности угроз: количественные, качественные.

ТЕМА 3.. Правовая защита информации. Иерархия нормативно-правовых актов. Система документов в области ЗИ. Конституция РФ о ЗИ. Доктрина информационной безопасности РФ. ФЗ РФ «Об информации, информационных технологиях и о защите информации», «О персональных данных», «О государственной тайне». Стандарты ИБ.

ТЕМА 4. Организация защиты информации
Принципы защиты информации. Методы и средства ЗИ.

ТЕМА 5. Физическая и программно-техническая защита информации.

Объекты технической защиты ИБ. Программные средства ЗИ. Аппаратные средства ЗИ. Инженерно-технические средства ЗИ. Требования по программно-технической защите информации.

ТЕМА 6. Криптографическая защита информации. Криптозащита и безопасные коммуникации: понятие криптографии, шифрование с помощью ключа, с симметричным ключом, асимметричное шифрование, шифрование с симметричным и асимметричным ключом. Безопасность при переписке. Определение цифровой подписи, законодательное регулирование, принцип действия. Цели ЭЦП. Организационные основы использования ЭЦП в информационных структурах. Правовые основы использования ЭЦП в информационных структурах.

ТЕМА 7. **Требования по обеспечению информационной безопасности.**

Подходы к разработке требований по обеспечению информационной безопасности. Политика информационной безопасности.

6. Методические материалы для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются самостоятельные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала.

Обучающемуся важно помнить, что лекция эффективно помогает ему овладеть программным материалом благодаря расстановке преподавателем необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации. Кроме того, во время лекции имеет место прямой визуальный и эмоциональный контакт обучающегося с преподавателем, обеспечивающий более полную реализацию воспитательной компоненты обучения.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности;
- совершенствование навыков применения процедур стандартизации, лицензирования и сертификации объектов и систем в области информационной безопасности,
– формирование навыков проведения экспериментальных исследований системы защиты информации;
– формирование навыков участия в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем и учитываются при аттестации студента.

Предметом «Информационная безопасность» являются методические и законодательные материалы по вопросам защиты информации. Значимость методических и законодательных материалов в области защиты информации и навыков работы с ними определяется тем, что вооружает специалиста знаниями об использовании методов и средств в области защиты информации. Знания методических и законодательных материалов позволяют правильно принимать участие в организации объекта информатизации по требованиям безопасности информации, принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации, принимать участие в проведении экспериментальных исследований системы защиты информации.

6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

Для очной формы обучения

№ п/п	Раздел (тема) дисциплины	Задание	Часы	Методические рекомендации по выполнению задания	Форма контроля
1	**2**	**3**	**4**	**5**	**6**
1.	Виды информации ограниченного доступа, понятие тайны	Выполнение задания по изучению видов тайн (конфиденциальной информации)	14	Изучение материала лекций, работа с литературой, нормативной	Устный опрос Проверка выполнения задания,

				базой СПП «Гарант», «Консультант+»	ответы на контрольные вопросы
2.	Классификация угроз безопасности информации	Выполнение задания по изучению угроз и методов оценки угроз	14	Изучение материала лекций, работа с литературой, нормативной базой СПП «Гарант», «Консультант+»	Устный опрос Проверка выполнения задания, ответы на контрольные вопросы
3.	Правовая защита информации	Задание по изучению нормативных и законодательных документов по защите информации.	14	Изучение материала лекций, работа с литературой, нормативной базой СПП «Гарант», «Консультант+»	Устный опрос Проверка выполнения задания, ответы на контрольные вопросы
4.	Организация защиты информации	Выполнить задание по изучению методов и средств защиты информации	14	Изучение материала лекций, работа с литературой, нормативной базой СПП «Гарант», «Консультант+»	Устный опрос Проверка выполнения задания, ответы на контрольные вопросы
5.	Физическая и программно-техническая защита информации	Задание по изучению объектов технической защиты информационной безопасности.	12	Изучение материала лекций, работа с литературой, нормативной базой СПП «Гарант», «Консультант+»	Устный опрос Проверка выполнения задания, ответы на контрольные вопросы
6	Криптографическая защита информации	Выполнение задания по изучению законодательного регулирования ЭЦП, принцип действия ЭЦП.	14	Изучение материала лекций, работа с литературой, нормативной базой СПП «Гарант», «Консультант+»	Устный опрос Проверка выполнения задания, ответы на контрольные вопросы
7	Требования по обеспечению информационной безопасности	Выполнить задание по изучению подходов к разработке требований по обеспечению информационной безопасности	22,75	Изучение материала лекций, работа с литературой, нормативной базой СПП	Устный опрос Проверка выполнения задания, ответы на

				«Гарант», «Консультант+»	контрольные вопросы
	Зачет		4		

6.2. Тематика и задания для практических занятий

ТЕМА 1.. Виды информации ограниченного доступа, понятие тайны.
Основные понятия дисциплины «Информационная безопасность». Законодательство ИБ. Виды информации ограниченного доступа: государственная тайна, конфиденциальная информация. Виды тайн (коммерческая, банковская, служебная, кредитной истории, тайна страхования, налоговая тайна, аудиторская тайна. Информация, к которой нельзя ограничивать доступ.

ТЕМА 2.. Классификация угроз безопасности информации.
Понятие угрозы информационной безопасности. Источники угроз. Классификации угроз ИБ. Методы оценки опасности угроз: количественные, качественные.

ТЕМА 3.. Правовая защита информации. Иерархия нормативно-правовых актов. Система документов в области ЗИ. Конституция РФ о ЗИ. Доктрина информационной безопасности РФ. ФЗ РФ «Об информации, информационных технологиях и о защите информации», «О персональных данных», «О государственной тайне». Стандарты ИБ.

ТЕМА 4. Организация защиты информации
Принципы защиты информации. Методы и средства ЗИ.

ТЕМА 5. Физическая и программно-техническая защита информации.

Объекты технической защиты ИБ. Программные средства ЗИ. Аппаратные средства ЗИ. Инженерно-технические средства ЗИ. Требования по программно-технической защите информации.

ТЕМА 6. Криптографическая защита информации. Криптозащита и безопасные коммуникации: понятие криптографии, шифрование с помощью ключа, с симметричным ключом, асимметричное шифрование, шифрование с симметричным и асимметричным ключом. Безопасность при переписке. Определение цифровой подписи, законодательное регулирование, принцип действия. Цели ЭЦП. Организационные основы использования ЭЦП в информационных структурах. Правовые основы использования ЭЦП в информационных структурах.

ТЕМА 7. **Требования по обеспечению информационной безопасности.**
Подходы к разработке требований по обеспечению информационной безопасности. Политика информационной безопасности.

6.3. Методические рекомендации студентам, изучающим дисциплину «Информационная безопасность»

Студенту настоятельно рекомендуется посещать лекции ввиду ограниченного количества литературы по данной тематике, постоянного обновления содержания лекций, большого объема наглядного и демонстрационного материала. Самостоятельная работа студента складывается из изучения материалов лекций и рекомендуемой литературы, подготовке к практическим занятиям по вопросам и заданиям, выданным преподавателям в конце лекции. Систематическая подготовка к практическим занятиям – залог накопления глубоких знаний и успешной сдачи зачета по дисциплине.

Самостоятельная работа студента складывается из изучения материалов лекций и рекомендуемой литературы, прочтения статей в периодических изданиях, написания

рефератов, подготовки аналитических обзоров, отчетов, решения задач по темам курса, подготовки к контрольной работе, подготовки к зачету.

Самостоятельная работа должна осуществляться по следующим направлениям:

- подготовка к практическим занятиям;
- подготовка к текущим контрольным мероприятиям (устные опросы, письменные отчеты);
- подготовка к промежуточным контрольным мероприятиям (блиц-опрос, тесты, решения задач);
- выполнение домашних индивидуальных заданий;
- другие виды работ.

Текущий контроль осуществляется в виде опросов по теории и нормативно-правовой базе. Промежуточный контроль включает также подготовка рефератов, презентаций, выступление с докладами по соответствующей теме.

В целях закрепления материала дисциплины студенты могут составить практические задачи, тесты, на любую из освоенных тем, которые оцениваются преподавателем на оценку. Этот вид работы не является обязательным, но его выполнение приносит студенту дополнительные оценки по дисциплине.

Самостоятельное изучение темы следует осуществлять, используя рекомендованную литературу. При возникновении трудностей и проблем в освоении темы следует воспользоваться консультацией с преподавателем.

Уровень и глубина усвоения дисциплины зависят от активной и систематической работы на лекциях, изучения рекомендованной литературы, выполнения контрольных письменных заданий.

7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

а) основная

1. Электронный документооборот и обеспечение безопасности стандартными средствами windows : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. – М. : КУРС, 2017. – 296 с. http://znanium.com/catalog.php?bookinfo=851088
2. Электронный документооборот и обеспечение безопасности стандартными средствами windows : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. – М. : КУРС, 2017. – 296 с. http://znanium.com/catalog.php?bookinfo=851088
3. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / А.Г. Фабричнов, А.С. Дёмушкин, Т.В. Кондрашова, Н.Н. Куняев. - Москва : Логос, 2011. - 452 с. - (Новая университетская библиотека). - ISBN 978-5-98704-541-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=84996
4. Информационное право : учебник для бакалавров / И. М. Рассолов [и др.] ; отв. ред. И.М. Рассолов. - Москва : Проспект, 2013. - 352 с. - (Учебники МГЮА для бакалавров). - УМО. - ОПД. - осн. - ISBN 978-5-392-10100-9 : 330.00.

б) дополнительная

1. Краснянский, М.Н. Проектирование информационных систем управления документооборотом научно-образовательных учреждений : монография / М.Н. Краснянский, С.В. Карпушкин, А.В. Остроух ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2015. - 216 с. : ил., табл., схем. - Биб-

лиогр. в кн.. - ISBN 978-5-8265-1477-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=444657
2. Защита конфиденциальной информации при электронном документообороте/МининИ.В., МининО.В. - Новосиб.: НГТУ, 2011. - 20 с.: ISBN 978-5-7782-1829-1 http://znanium.com/catalog.php?bookinfo=546492
3. Мухин, Н.П. Компьютерные системы управления документооборотом / Н.П. Мухин. - Москва : Лаборатория книги, 2010. - 58 с. : ил., табл. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=87235
4. Рассолов, И. М. Информационное право : учебник для магистров / Рассолов Илья Михайлович. - 2-е изд., испр. и доп. - Москва : Юрайт, 2015; 2013. - 448 с. - (Магистр). - МО РФ. - осн. - ISBN 978-5-9916-2709-2 : 499.00; 433.00.

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

Информационно-образовательные ресурсы:

1. www.atlas.Krasnodar.ru -КФ НТЦ «Атлас»: защита информации.

Электронные библиотечные системы:

1. Университетская библиотека онлайн http://biblioclub.ru
2. «Лань» http://e.lanbook.com/
3. ЭБС «Znanium»
4. Справочно-информационная система (СИС) «Гарант».
5. Справочно-информационная система «Консультант».
6.Электронно-библиотечная система (ЭБС) «Инфра-М».

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

Мультимедийный комплекс, включающий электронную доску, ноутбук и проектор.