

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Костромской государственный университет»
(КГУ)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление 38.03.01 Экономика Профиль Финансы и кредит

Направленность/специализация: Финансы и кредит

Квалификация выпускника: Бакалавр

Кострома
2021

Рабочая программа дисциплины «Информационная безопасность» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 38.03.01 Экономика (приказ Минобрнауки России от 12 августа 2020 г. № 954)

Разработал: Щекочихин О.В., зав. кафедрой защиты информации, к.т.н., доцент
без подписи

Рецензенты: Замураев Игорь Николаевич

Директор департамента финансов
Костромской области

Рецензенты: Иванов Алексей Александрович

Заместитель управляющего
Костромским ГОСБ №8640 ПАО
Сбербанк

ПРОГРАММА УТВЕРЖДЕНА:

На заседании кафедры теоретической и прикладной экономики, финансов и кредита КГУ,

Протокол заседания кафедры № 8 от 19.05.2021 г.

Заведующий кафедрой теоретической и прикладной экономики, финансов и кредита КГУ,

Шумакова Ольга Данииловна, к.э.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры _____:

Протокол заседания кафедры №__ от _____20__г.

(ФИО), ученая степень, ученое звание

1. Цели и задачи освоения дисциплины

Цель дисциплины: Целью изучения дисциплины является ознакомление студентов с: основными понятиями и определениями информационной безопасности; угрозами, которыми подвергается информация; вредоносными программами. защитой от компьютерных вирусов и других вредоносных программ; методами и средствами защиты информации; защитой информации в сетях;

Задачи дисциплины:

ознакомить студентов с тенденциями развития защиты информации, с терминологией и основными понятиями теории защиты информации, а так же с методами защиты компьютерной информации

- основным понятиям и определениям информационной безопасности;
- противостоять угрозам, которым подвергается информация;
- защите от вредоносных программ и компьютерных вирусов;
- методам и средствам защиты информации в компьютерных сетях

2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

В совокупности с другими базовыми дисциплинами обеспечивает формирование следующих компетенций:

Освоить компетенцию:

ПК-3Способность рассчитывать, анализировать и интерпретировать информацию, необходимую для выявления тенденций развития финансового рынка и осуществления консультирования его участников, в том числе на основе зарубежного опыта

Код и содержание индикаторов компетенции:

ИК. ПК3.1.1. Владеет методами анализа и оценки рисков деятельности организаций, в том числе, кредитно-финансовых и предлагает решения по их минимизации в целях достижения финансовой стабильности.
ИК. ПК-3.2. Применяет финансовые инструменты для минимизации потерь финансово-кредитных институтов, иных организаций различных отраслей экономики, финансовых органов государственного сектора.
ИК. ПК-3.3. Демонстрирует знание зарубежного опыта регулирования финансово-кредитной сферы и ее институтов в целях достижения финансовой стабильности и обеспечения экономического роста.

Знать:

- **Общие вопросы обеспечения информационной безопасности банка**
- основные понятия и определения информационной безопасности;
- методы противостояния угрозам, которым подвергается информация;
- способы защиты от вредоносных программ и компьютерных вирусов;
- методы и средства защиты информации в компьютерных сетях.

Уметь:

- выявлять источники, риски и формы атак на информацию,
- участвовать в разработке политики защиты конфиденциальной информации в соответствии с российским законодательством,

Владеть:

- **Современными методами получения, анализа, обработки информации**
- Методами защиты конфиденциальной информации

3. Место дисциплины в структуре ОП ВО

Дисциплина относится к части учебного плана формируемой участниками образовательных отношений. Изучается в 3 семестре очной, очно-заочной и заочной формы обучения.

Изучение дисциплины основывается на ранее освоенных дисциплинах/практиках: Информационные системы в экономике и управлении; Цифровая экономика и финансовая грамотность

Изучение дисциплины является основой для освоения последующих дисциплин/практик: Профессиональные компьютерные программы, Основы цифрового маркетинга

Компетенция ПК 10 осваивается так же на следующих дисциплинах:

Б1.В.04	Финансы
Б1.В.07	Анализ больших данных
Б1.В.09	Деньги, кредит, банки
Б1.В.12	Финансовый механизм государственных закупок
Б1.В.15	Финансовый риск-менеджмент
Б1.В.17	Финансовые рынки
Б1.В.20	Практикум по подготовке специалиста для работы на рынке ценных бумаг и фондовой бирже
Б1.В.23	Международные валютно-кредитные и финансовые отношения
Б1.В.24	Основы банковского менеджмента
Б1.В.ДВ.04.01	Инвестиционное проектирование
Б1.В.ДВ.04.02	Инвестиционные стратегии
Б1.В.ДВ.08.01	Поведенческие финансы
Б1.В.ДВ.08.02	Технический анализ на фондовом рынке
Б2.В.01(П)	Технологическая (проектно-технологическая) практика
Б2.В.02(П)	Преддипломная практика
Б3.01(Г)	Подготовка к сдаче и сдача государственного экзамена
Б3.02(Д)	Подготовка к процедуре защиты и защита выпускной квалификационной работы

4. Объем дисциплины

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

Виды учебной работы,	Очная форма	Очно-заочная	Заочная
Общая трудоемкость в зачетных единицах	3	3	3
Общая трудоемкость в часах	108	108	108
Аудиторные занятия в часах, в том числе:			
Лекции	16	10	10
Практические занятия	16	12	12
Лабораторные занятия	-	-	-
Практическая подготовка	-		
Самостоятельная работа в часах	75,75	85,75	85,75
Форма промежуточной аттестации	Зачет	Зачет	Зачет

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма	Очно-заочная	Заочная
Лекции	16	10	10
Практические занятия	16	12	12
Лабораторные занятия	-	-	-

Консультации	-	-	-
Зачет/зачеты	0,25	0,25	0,25
Экзамен/экзамены	-		
Курсовые работы	-		
Курсовые проекты	-		
Практическая подготовка	-		
Всего	32,25	22,25	22,25

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

5.1 Тематический план учебной дисциплины

Очная форма обучения

№	Название раздела, темы	Всего з.е/час	Аудиторные занятия			Самостоятельная работа
			Лекц.	Практ.	Лаб.	
1	Раздел 1. Организационные и правовые основы информационной безопасности	32	6	6		20
1.1	Понятие цифровой экономики и компетенции в эпоху цифровой экономики	10	2	2		6
1.2	Значение информационной безопасности и её место в кредитно-финансовой системе	12	2	2		6
1.3	Базовое законодательство в области информационных технологий и защиты информации. Стандарты в области информационной безопасности. Требования к безопасности управления данными и предотвращение утечек данных из финансовых организаций	12	2	2		8
2	Раздел 2. Угрозы информационной безопасности	28	4	4		20
2.1	Угрозы информационной	14	2	2		10

	безопасности					
2.2	Виды атак на информационную систему	14	2	2		10
3	Раздел 3. Способы и методы защиты информации	32	6	6		20
3.1	введение требований к устойчивости и бесперебойности деятельности финансовых организаций при реализации киберрисков	12	2	2		8
3.2	киберкультуры финансового рынка.	10	2	2		6
3.3	Технические методы защиты информации	10	2	2		6
	зачет					15,75
	Итого:	3/108	16	16		75,75

Очная-заочная и заочная форма обучения

№	Название раздела, темы	Всего з.е/час	Аудиторные занятия			Самостоятельная работа
			Лекц.	Практ.	Лаб.	
1	Раздел 1. Организационные и правовые основы информационной безопасности	28	4	4		20
1.1	Понятие цифровой экономики и компетенции в эпоху цифровой экономики	18	1	1		6
1.2	Значение информационной безопасности и её место в кредитно-финансовой системе	18	1	1		6
1.3	Базовое законодательство в области информационных технологий и защиты информации. Стандарты в области информационной безопасности. Требования к безопасности управления данными и предотвращение	12	2	2		8

	утечек данных из финансовых организаций					
2	Раздел 2. Угрозы информационной безопасности	26	2	4		20
2.1	Угрозы информационной безопасности	13	1	2		10
2.2	Виды атак на информационную систему	13	1	2		10
3	Раздел 3. Способы и методы защиты информации	38	4	4		30
3.1	введение требований к устойчивости и бесперебойности деятельности финансовых организаций при реализации киберрисков	14	2	2		10
3.2	киберкультуры финансового рынка.	12	1	1		10
3.3	Технические методы защиты информации	12	1	1		10
	зачет					15,75
	Итого:	3/108	10	12		85,75

5.2. Содержание:

Раздел 1. Организационные и правовые основы информационной безопасности. Актуальность информационной безопасности. Национальные интересы РФ в информационной сфере и их обеспечение. Понятие цифровой экономики и компетенции в эпоху цифровой экономики, Значение информационной безопасности и её место в кредитно-финансовой системе, Базовое законодательство в области информационных технологий и защиты информации. Стандарты в области информационной безопасности. Требования к безопасности управления данными и предотвращение утечек данных из финансовых организаций, Классификация компьютерных преступлений. Способы совершения компьютерных преступлений. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet. Понятия и определения в информационной безопасности.

Раздел 2. Угрозы информационной безопасности Угрозы информационной безопасности, Виды атак на информационную систему, Виды угроз информационной безопасности. Источники угроз информационной безопасности. Условия существования вредоносных программ. Классические компьютерные вирусы. Сетевые черви. Троянские программы. Спам. Хакерские утилиты и прочие вредоносные программы. Кто и почему создает вредоносные программы.

Раздел 3. Способы и методы защиты информации.

Введение требований к устойчивости и бесперебойности деятельности финансовых организаций при реализации киберрисков, киберкультуры финансового рынка, Технические методы защиты информации, Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы. Методы обеспечения информационной безопасности. Ограничение доступа. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Выбор средств информационной защиты. Стандарты безопасности. Критерии безопасности банковских систем.

6. Методические материалы для обучающихся по освоению дисциплины

6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

Для очной, очно-заочной и заочной формы обучения раздел заполняются отдельно.

№ п/п	Раздел (тема) дисциплины	Задание	Часы Очная форма	Часы очно- заочная, заочная	Методические рекомендации по выполнению задания	Форма контроля
1	Раздел 1. Организационные и правовые основы информационной безопасности.	Изучение литературы и Интернет-источников	20	20	В качестве литературных источников предпочтительнее использовать [2] из списка дополнительной литературы и [1, 3] из списка основной литературы	Проверка
2	Раздел 2. Угрозы информационной безопасности	Изучение литературы и Интернет-источников	20	20	В качестве литературных источников предпочтительнее использовать [2] из списка дополнительной литературы и [1, 3] из списка основной литературы	Тестирование
3	Раздел 3. Способы и методы защиты информации.	Составление программ	20	30	Для подготовки к составлению программ рекомендуется пользоваться учебными пособиями [2] из списка основной литературы и [1] из списка дополнительной литературы	Контрольная

4	Зачет	Решение зачетных заданий	15,75	15,75	Для подготовки к составлению программ рекомендуется пользоваться учебными пособиями [2] из списка основной литературы и [1] из списка дополнительной литературы	Зачет
---	-------	--------------------------	-------	-------	---	-------

6.2. Тематика и задания для практических занятий

1. Подписание документа электронной подписью, проверка электронной подписи документа
2. Анализ угроз информационной системы финансового сектора
3. Анализ нормативно-правовой базы по защите информации в кредитно-финансовой сфере
4. Построение модели нарушителя информационной безопасности
5. Построение модели угроз
6. Построение модели информационной безопасности организации кредитно-финансовой сферы

Темы докладов на практических занятиях

1. Форензика.
2. Угрозы информационной безопасности соц. Сетей.
3. История компьютерных вирусов. Крупнейшие атаки вирусов.
4. История развития антивирусов. Архитектура современного антивируса.
5. Крупнейшие компании мирового рынка безопасности.
6. Известные хакеры и хакерские группировки. Преступления и наказания.
7. Тестирование на проникновение как метод практического аудита информационной безопасности
8. Перспективные направления развития методов и средств защиты информации.
9. Прогнозы известных футуристов и писателей фантастов сценариев развития цифрового общества, систем контроля и безопасности
10. Виртуальная и дополненная реальность угрозы и возможности развития

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

а) основная

1. **Информационная безопасность конструкций ЭВМ и систем** : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. — М. : ИНФРА-М, 2018. — 118 с. + Доп. материалы [Электронный ресурс; Режим доступа <http://www.znanium.com>]. — (Высшее образование: Бакалавриат). — <http://znanium.com/catalog.php?bookinfo=925825>

2. **Информационная безопасность и защита информации:** Учебное пособие. / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2017. — 322 с. — (Высшее образование). — <http://znanium.com/catalog.php?bookinfo=763644>
3. **Загинайлов, Ю.Н.** Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>
4. **Нестеров, С.А.** Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - Санкт-Петербург. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=363040>
5. **Информационная безопасность и защита информации :** учеб. пособие для вузов / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2010. - 384 с.: рис. - ISBN 978-5-94178-216-1 : 590.00.
6. **Бабаш, Александр Владимирович .**
Информационная безопасность: Лабор. практикум+CD: учеб. пособие / Бабаш, Александр Владимирович . - 2-изд., стер. - Москва :КноРус, 2013. - 136 с.: рис. - (Бакалавриат). - СД. - осн. - ISBN 978-5-406-02760-8 : 303.00.

б) дополнительная

1. **Информационная безопасность предприятия :** учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). <http://znanium.com/catalog.php?bookinfo=612572>
2. **Информационная система предприятия:** Учебное пособие/Вдовенко Л. А., 2-е изд., пераб. и доп. - М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. - 304 с.: 60x90 1/16 (Переплёт 7БЦ) ISBN 978-5-9558-0329-6, 500 экз.
<http://znanium.com/catalog.php?bookinfo=501089>
3. **Артемов, А.В.** Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=428605>
4. **Золотарев, В. В.** Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие/ В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с.
<http://znanium.com/catalog.php?bookinfo=463037>
5. **Жукова, М. Н.**Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. <http://znanium.com/catalog.php?bookinfo=463061>
6. **Бабаш, Александр Владимирович.**
Информационная безопасность : лабораторный практикум : учеб. пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - М. : КНОРУС, 2012. - 131 с. + 1 опт. диск. - Библиогр.: с. 131. - ISBN 978-5-406-01170-6 : 250.00.
7. **Мельников, Владимир Павлович.**
Информационная безопасность и защита информации : учеб. пособие для вузов спец. 230201 "Информац. системы и технологии" / Мельников Владимир Павлович, С. А. Клейменов, А. М. Петраков ; под ред. Клейменова С.А. - 3-е изд., стер. - Москва : Академия, 2008. - 336 с. - (Высш. проф. образов. Информат. ивыч. техн.). - УМО. - ЕН, ОПД, СД. - ISBN 978-5-7695-4884-0 : 165.66.
8. **Партыка, Татьяна Леонидовна.**
Информационная безопасность : Учеб. пособие для сред. проф. образования, спец. информатики и выч. техники / Партыка Татьяна Леонидовна, Попов Игорь Иванович. - 2-е изд., испр. и доп. - Москва : ФОРУМ - ИЕФРА-М, 2007. - 368 с.: ил. -

(Профессиональное образование). - МО РФ . - ОПД, СД. - ISBN 5-91134-095-X; 5-16-002849-8 : 288.00.

9. Филин, Сергей Александрович.

Информационная безопасность : учеб. пособие / Филин Сергей Александрович. - Москва : Альфа-Пресс, 2006. - 412 с. - ОПД, СД. - ISBN 5-94280-163-0 : 200.00.

10. Малюк, А. А.

Информационная безопасность: концептуальные и методологические основы защиты информации : Учеб. пособие для студ. высш. учеб. заведений / А. А. Малюк. - М. : Горячая линия-Телеком , 2004. - 280 с. : ил. - Библиогр.: с. 276-278. - ISBN 5-93517-197-X : 99.00.

В прил.: Гос. образовательный стандарт высшего профессионального образования. - Допущено МО РФ

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

Информация о курсе дисциплины в СДО:

Элемент «Лекции»;

Элемент «Практические задания»;

Информационно-образовательные ресурсы:

1. Библиотека ГОСТов. Все ГОСТы, [Электронный ресурс], URL:<http://vsegost.com/>
2. 1. www.atlas.Krasnodar.ru -КФ НТЦ «Атлас»: защита информации.

Электронные библиотечные системы:

1. ЭБС Университетская библиотека онлайн - <http://biblioclub.ru>
2. ЭБС «Лань» <https://e.lanbook.com>
3. ЭБС «ZNANIUM.COM» <http://znanium.com>
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

Лекционные занятия проводятся в аудиториях с требуемым числом посадочных мест, оборудованные мультимедиа.

Практические занятия проводятся в компьютерных классах.

Лицензионное программное обеспечение:

Не требуется

Свободно распространяемое программное обеспечение:

Офисный пакет