АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
ИНСТИТУТ ЭКОНОМИКИ И УПРАВЛЕНИЯ В ПРОМЫШЛЕННОСТИ
Экономический факультет
Кафедра Экономики

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность»

38.03.05 «Бизнес-информатика» (профиль – «Цифровая экономика»)

Квалификация выпускника: бакалавр

Форма обучения: *очно-заочная, заочная*

Год начала подготовки: 2023

Москва, 2023 г.

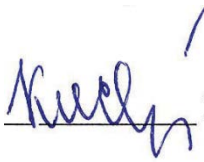
Программу подготовил(и):
Бахметьев В.А.

Рабочая программа дисциплины
«Информационная безопасность»

разработана в соответствии с ФГОС ВО:

1. Федеральный государственный стандарт высшего образования – бакалавриат по направлению подготовки 38.03.05 «Бизнес-информатика» (Приказ Министерства науки и высшего образования РФ от 29 июля 2020 г. N 838 "Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 38.03.05 Бизнес-информатика" (с изменениями и дополнениями), зарегистрирован Министерством юстиции Российской Федерации 19 августа 2020 г. Регистрационный N 59325) составлена на основании учебного плана: Бизнес-информатика, профиль «Цифровая экономика»;
2. Профессиональный стандарт 06.016 «Руководитель проектов в области информационных технологий» (приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 № 893н.).

Рабочая программа одобрена на заседании кафедры **Экономика**
Протокол от 27 февраля 2023 г. №7

Зав. кафедрой  **Киселев В.В.**

1. Цели освоения дисциплины

Целью освоения учебной дисциплины «Информационная безопасность» является формирование у обучающихся общекультурных и профессиональных компетенций в процессе изучения различных аспектов защиты информации для последующего применения в учебной и практической деятельности. Содержательно-методическая специфика программы предполагает рассмотрение широкого ряда экономико-правовых вопросов с учётом особенностей IT-сферы.

Задачи дисциплины:

- систематизация, формализация и расширение знаний по основным
- положениям теории информации, информационной безопасности и стандартами шифрования;
- изучение математических основ защиты информации; а также методов, средств и инструментов шифрования, применяемых в сфере информационных технологий и бизнеса;
- дать студенту достаточно прочные представления о информационной безопасности, включая аппаратную часть и математическое обеспечение;
- привитие навыков работы с методами шифрования и криптоанализа;
- формирование современной культуры программирования.

2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.11 относится к части, формируемой участниками образовательных отношений, базового учебного плана образовательной программы по направлению «Бизнес-информатика».

Освоение дисциплины «Информационная безопасность» базируется на знаниях, полученных после изучения курсов «Базы данных», «Жизненный цикл ИС», «Управление IT-сервисом и контентом», «Введение в специальность», «Информационные технологии в экономике» и «Экономическая информатика»

Освоение необходимо студентам для успешного прохождения преддипломной практики в организации IT-профиля и дальнейшей профессиональной деятельности в IT-бизнесе.

Дисциплина изучается на 5 курсе, в 9 семестре.

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

В результате освоения дисциплины обучающийся должен продемонстрировать следующие результаты:

Компетенция	Индикаторы	Перечень планируемых результатов обучения по дисциплине
ПК-1 Способен осуществлять мониторинг, анализ, систематизацию и обработку информации о	*ИПК-1.1 Умеет мыслить системно, структурировать информацию* *ИПК-1.3 Проводит информационно-аналитическую работу по рынку информационных продуктов и услуг, прогнозирует изменения информационного рынка*	**Знать:** - математические принципы, лежащие в основе криптографических моделей; - теорию простых чисел и модульной арифметики - основные принципы административно- правовой защиты информации **Уметь:** -уметь использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования; - уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач - быстро реагировать на различные угрозы

информационных системах в соответствии с полученным планом	.	информационной безопасности уметь применять современные технологии создания брандмауэров и IDS-комплексов **Владеть:** - алгоритмическими языками для разработки прикладных алгоритмов шифрования; владеть навыками решения задач криптоанализа и шифрования; - приемами обнаружения сетевых проникновений - навыками применения, установки и настройки антивирусных систем и систем распознавания угроз и атак; - навыками работы по обнаружению и защите от DDOS-атак

4. 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

Общая трудоемкость (объем) дисциплины составляет 6 зачетных единицы, 216академических часа.

На лекционные занятия отводится 16 часов по очно-заочной форме и 12 часа по очной форме обучения.

На занятия семинарского типа (практические занятия) отводится 20 часов по очно-заочной и 20 часа по заочной форме обучения.

На самостоятельную работу (без учёта подготовки к экзамену) отводится 171 и 175 часов соответственно.

На подготовку к экзамену отводится 9 часов.

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Тематические разделы дисциплины и компетенции, которые формируются при их изучении

№ п/п	Наименование раздела дисциплины	Содержание раздела	Код формируемой компетенции
1	Основные составляющие информационной безопасности	Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности	ПК-1
2	Криптографические способы защиты ин формации	Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и	ПК-1

		матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Одноалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA	
3	Антивирусная защита	Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы	ПК-1
4	Сетевая безопасность	Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил	ПК-1

		межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS	

5.2. Разделы дисциплины, виды учебных занятий и формы текущего контроля успеваемости по очно-заочной форме

№	Наименование раздела дисциплины	Трудоемкость в часах					Формы СРС	Формы текущего контроля с указанием баллов (при использовании балльной системы оценивания)
		Всего (вкл. СРС)	На контактную работу по видам учебных занятий			На СРС		
			Л	ПЗ	ИЗ			
1	Основные составляющие информационной безопасности	52	4	6		42	Реферирование литературы	Опрос контрольная
2	Криптографические способы защиты ин формации	52	4	4		44	Реферирование литературы	Опрос контрольная
3	Антивирусная защита	52	4	6		42	Реферирование литературы	Опрос контрольная
4	Сетевая безопасность	51	4	4		43	Реферирование литературы	Опрос контрольная
	Экзамен	9						
ИТОГО:		216	16	20		99		

5.3. Разделы дисциплины, виды учебных занятий и формы текущего контроля успеваемости по очно-заочной форме

№	Наименование раздела дисциплины	Трудоемкость в часах					Формы СРС	Формы текущего контроля с указанием баллов (при использовании балльной системы
		Всего (вкл. СРС)	На контактную работу по видам учебных занятий			На СРС		
			Л	ПЗ	ИЗ			

								оценивания)
1	Основные составляющие информационной безопасности	52	4	6		42	Реферирование литературы	Опрос контрольная
2	Криптографические способы защиты ин формации	52	4	4		44	Реферирование литературы	Опрос контрольная
3	Антивирусная защита	52	2	6		44	Реферирование литературы	Опрос контрольная
4	Сетевая безопасность	51	2	4		45	Реферирование литературы	Опрос контрольная
	Экзамен	9						
ИТОГО:		216	12	20		175		

6. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

№	Наименование раздела дисциплины	Содержание СРС	Контроль
1	Основные составляющие информационной безопасности	работа с пройденным материалом по конспектам лекций и учебнику. Доклады.	Сдается преподавателю в электронном виде
2	Криптографические способы защиты ин формации	работа с пройденным материалом по конспектам лекций и учебнику. Доклады.	Сдается преподавателю в электронном виде
3	Антивирусная защита	работа с пройденным материалом по конспектам лекций и учебнику. Доклады. Кейсы	Сдается преподавателю в электронном виде
4	Сетевая безопасность	работа с пройденным материалом по конспектам лекций и учебнику. Доклады. Кейсы	Сдается преподавателю в электронном виде

7. Проведение промежуточной аттестации обучающихся по дисциплине

7.1. Общие условия

Промежуточная аттестация проводится в 9 семестре в форме устного экзамена.

7.2. Критерии и шкалы оценивания результатов обучения по дисциплине

Код компетенции	Показатели достижения результатов обучения	Критерии и шкала оценивания				Перечень оценочных средств
		Отлично	**Хорошо**	**Удовл**	**Неудовл.**	
ПК-1. Способен	*ИПК-1.1 Умеет мыслить системно, структурирова*	Ответы на поставленные вопросы в билете	Ответы на поставленные вопросы излагаются	Допускаются нарушения в	Материал излагается непоследовательно,	Тесты Рефераты Практические

осуществлять мониторинг, анализ, систематизацию и обработку информации о информационных системах в соответствии с полученным планом	*ть информацию* *ИПК-1.3 Проводит информационно-аналитическую работу по рынку информационных продуктов и услуг, прогнозирует изменения информационного рынка*	излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстрируются глубокие знания базовых нормативно-правовых актов. Соблюдаются нормы литературной речи.	систематизировано и последовательно. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи.	последовательности изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи. Отмечается слабое владение терминологией.	сбивчиво, не представляет определенной системы знаний по дисциплине. Имеются заметные нарушения норм литературной речи.	задачи

7.3. Оценочные средства для промежуточной аттестации

Задания для индивидуального выполнения

1. Основные понятия информационной безопасности. Классификация угроз.
2. Целостность и конфиденциальность. Классификация средств защиты информации.
3. Базовые понятия теории информации.
4. Методы и средства инженерно-технической защиты.
5. Модель сетевой безопасности. Классификация сетевых атак.
6. Простые криптосистемы. Шифрование методом замены (подстановки): Одноалфавитная подстановка;
7. Простые криптосистемы. Шифрование методом замены (подстановки): Многоалфавитная многоконтурная подстановка.
8. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам
9. Стандарт шифрования данных RSA
10. Основные приемы криптоанализа при симметричных ключах.
11. Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты сети.
12. Конфигурация межсетевого экрана. Построение набора правил межсетевого экрана для различных типов архитектуры

8. Перечень образовательных технологий

В процессе преподавания дисциплины используются следующие образовательные технологии:

1. Лекция - диалог
2. Лекция-дискуссия

3. Решение ситуационных заданий
4. Форма конференции

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

а) Основная литература

1. Фомин, Д. В. Информационная безопасность : учебник / Д. В. Фомин. — Москва : Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/118876.html

2. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. — Москва, Вологда : Инфра-Инженерия, 2022. — 104 с. — ISBN 978-5-9729-0864-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/124242.html

3. Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет : учебное пособие / Ю. А. Семенов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 581 с. — ISBN 978-5-4497-1653-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/120489.html

б) Дополнительная литература

1. Попова, Г. Л. Информационная экономика : учебное пособие / Г. Л. Попова. — Москва : Ай Пи Ар Медиа, 2022. — 117 с. — ISBN 978-5-4497-1578-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/118877.html

2. Информационный менеджмент : учебное пособие / Е. В. Ильина, А. И. Романова, О. В. Бахарева [и др.]. — Москва : Ай Пи Ар Медиа, 2022. — 98 с. — ISBN 978-5-4497-1381-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/116446.html

   Елкина, О. С. Экономическая безопасность предприятия (организации) : учебник / О. С. Елкина. — Москва : Ай Пи Ар Медиа, 2022. — 313 с. — ISBN 978-5-4497-1417-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/116247.html

10. Перечень ресурсов информационно-телекомуникационной сети «Интернет», профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

1. http://aup.ru - Административно-управленческий портал
2. http://www.elibrary.ru – цифровая научная библиотека
3. http://www.cyberleninka.ru – цифровая научная библиотека
4. https://www.it-world.ru/ - портал о цифровых технологиях

5. https://securitymedia.org/ - новости информационной безопасности

11. Методические указания для обучающихся по освоению дисциплины

Изучение учебной дисциплины «Бизнес-информатика» предполагает овладение материалами лекций, учебника, программы, работу студентов в ходе проведения практических занятий, а также систематическое выполнение письменных работ в форме рефератов, тестовых и иных заданий для самостоятельной работы студентов.

В ходе лекций раскрываются основные вопросы в рамках рассматриваемого раздела, делаются акценты на наиболее сложные и интересные положения изучаемого материала, которые должны быть приняты студентами во внимание. Материалы лекций являются основой для подготовки студента к практическим занятиям и выполнения заданий самостоятельной работы.

Основной целью практических занятий является контроль за степенью усвоения пройденного материала, ходом выполнения студентами самостоятельной работы и рассмотрение наиболее сложных и спорных вопросов.

12. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Для проведения занятий лекционного и семинарского типа предлагаются мультимедийные средства: видеопроектор, ноутбук, экран настенный, др. оборудование или компьютерный класс.

Операционная система – Linux, пакет офисных программ – LibreOffice либо операционная система – Windows, пакет офисных программ – Microsoft Office в зависимости от распределения аудиторий. Учебные аудитории оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Института.

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

Для изучения дисциплины «Бизнес-информатика» необходимо наличие аудитории, оснащённой мультимедийными средствами обучения для чтения лекций и проведения семинарских занятий.