

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского»**

Институт экономики и предпринимательства

УТВЕРЖДЕНО
решением ученого совета ННГУ
протокол от
«14» декабря 2021 г. № 4

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень высшего образования
бакалавриат

Направление подготовки
38.03.01 Экономика

Направленность образовательной программы
Мировая экономика (на английском языке)

Форма обучения
очная

Нижегород

2021 год

1. Место дисциплины в структуре ООП

Дисциплина Б1.О.15 «Информационная безопасность» относится к обязательной части.

Место дисциплины в учебном плане образовательной программы	
Блок 1. Дисциплины (модули) Обязательная часть	Дисциплина Б1.О.15 «Информационная безопасность» относится к обязательной части ООП направления подготовки 38.03.01 «Экономика»

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции* (код, содержание индикатора)	Результаты обучения по дисциплине**	
ОПК-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК 6.1. Понимает принципы работы современных информационных технологий	Знать: современные коды шифрования Уметь: реагировать на инциденты Владеть: навыками анализа рисков	Задачи, тест, дискуссия
	ОПК 6.2. Использует принципы работы современных информационных технологий для решения задач профессиональной деятельности	Знать: типы атак, методы обеспечения безопасности приложений Уметь: работать с моделями безопасности системы Владеть: обеспечением инфраструктурных услуг	Задачи, тест, дискуссия
ПК-3. Способен анализировать и интерпретировать данные отечественной и зарубежной финансовой, бухгалтерской и иной информации, выявлять тенденции изменения экономических и социально-экономических показателей и использовать полученные сведения для принятия управленческих решений	ПК 3.1. Формирует, анализирует и интерпретирует финансово-экономическую информацию	Знать: бизнес-процессы и технический контроль Уметь: планировать непрерывность бизнеса. Владеть: практическими навыками безопасности соединений	Задачи, тест, дискуссия
	ПК 3.2. Выявляет тенденции и использует результаты анализа информации для принятия управленческих решений	Знать: тенденции развития систем безопасности хранения данных, общие концепции безопасности баз данных Уметь: проектировать системы безопасности в сети Владеть: навыками аутентификации и управления персоналом	Задачи, тест, дискуссия

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения
Общая трудоемкость	4 ЗЕТ
Часов по учебному плану	144
в том числе	
аудиторные занятия (контактная работа):	
- занятия лекционного типа	16
- занятия семинарского типа (практические занятия)	16
самостоятельная работа	56
КСР	2
Промежуточная аттестация – Экзамен - 54	

3.2. Содержание дисциплины

Modules or topics	Workload (hours)	Including				
		Contact Work				Independent work
		Lectures	Seminars	Lab classes	Total	
Тема 1	11	2	2		4	7
Тема 2	11	2	2		4	7
Тема 3	11	2	2		4	7
Тема 4	11	2	2		4	7
Тема 5	11	2	2		4	7
Тема 6	11	2	2		4	7
Тема 7	11	2	2		4	7
Тема 8	11	2	2		4	7
Текущий контроль	2					
Экзамен	54					
Итого	144	16	16		32	56

Содержание курса:

Тема 1. Основы. Обзор информационной безопасности. Анализ рисков. Соблюдение стандартов, правил и законов. Принципы безопасного проектирования.

Тема 2. Политика безопасности. Стандарты, процедуры и руководящие принципы. Организация безопасности. Аутентификация и авторизация.

Тема 3. Безопасность данных. Защита неструктурированных данных. Управление правами на информацию. Шифрование. Безопасность хранения. Безопасность базы данных.

Тема 4. Сетевая безопасность. Дизайн защищенной сети. Безопасность сетевых устройств. Брандмауэры. Виртуальные частные сети. Безопасность беспроводной сети. Системы обнаружения и предотвращения вторжений. Безопасность передачи голоса по IP (VoIP) и АТС.

Тема 5. Компьютерная безопасность. Модели безопасности операционной системы. Безопасность Unix. Безопасность Windows. Обеспечение безопасности инфраструктурных услуг. Виртуальные машины и облачные вычисления. Защита мобильных устройств.

Тема 6. Безопасность приложений. Безопасный дизайн приложения. Написание защищенного программного обеспечения. Безопасность J2EE. Сетевая безопасность Windows. Управление поведением приложения.

Тема 7. Операции по обеспечению безопасности. Управление операциями безопасности. Аварийное восстановление, непрерывность бизнеса, резервное копирование и высокая доступность. Реагирование на инциденты и судебно-медицинский анализ.

Тема 8. Физическая безопасность. Классификация активов. Оценка физической уязвимости. Выбор местоположения сайта для обеспечения безопасности. Соответствие стандартам.

Практические занятия (семинарские занятия) организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка предполагает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных программ, деловых игр, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В рамках данного курса возможны встречи с представителями компаний различных форм собственности, государственных и муниципальных органов.

Практическая подготовка направлена на формирование и развитие:

- практических навыков в соответствии с профилем ОП: *аналитической деятельности и компетенции ПК-3*: Способен анализировать и интерпретировать данные отечественной и зарубежной финансовой, бухгалтерской и иной информации, выявлять тенденции изменения экономических и социально-экономических показателей и использовать полученные сведения для принятия управленческих решений.

Текущий контроль успеваемости реализуется в рамках занятий семинарского типа, групповых или индивидуальных консультаций.

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

В ходе изучения дисциплины уделяется внимание как теоретическому усвоению понятий информационной безопасности, так и приобретению, развитию и закреплению практических навыков и умений по использованию специализированных информационных средств и технологий при организации ИБ экономических систем.

На лекциях раскрываются основные вопросы рассматриваемой темы, делаются акценты на наиболее важные, сложные и проблемные положения изучаемого материала, которые должны быть приняты студентами во внимание.

На практических занятиях, ориентированных на предметную область будущей профессиональной деятельности студентов, выборочно контролируется степень усвоения студентами основных теоретических положений. Рассматривается технология применения аппаратно-программных средств для организации ИБ. При решении практических заданий используются не только инструментальные средства информационных технологий бизнес-индустрии, но и методы и понятия дисциплин финансово-экономического блока.

После изучения каждой темы предусматривается выполнение студентами самостоятельной работы с проверкой как степени усвоения ими теоретических, знаний, так и объема и качества приобретенных практических навыков и умений.

В ходе самостоятельной работы, при подготовке к плановым занятиям, экзамену студенты анализируют поставленные преподавателем задачи и проблемы и с использованием учебно-методической литературы, информационных систем, комплексов и технологий, материалов, найденных в глобальной сети Интернет, находят пути их разрешения.

Для достижения поставленных целей преподавания дисциплины реализуются следующие средства, способы и организационные мероприятия:

- изучение теоретического материала дисциплины на лекции с использованием компьютерных технологий;
- самостоятельное изучение теоретического материала дисциплины с использованием Internet-ресурсов, информационных баз, методических разработок, специальной и научной литературы;
- закрепление теоретического материала при проведении практических занятий с использованием учебного и научного оборудования, выполнения проблемно-ориентированных, поисковых, творческих заданий.

Самостоятельная работа является наиболее деятельным и творческим процессом, который выполняет ряд дидактических функций: способствует формированию диалектического мышления, вырабатывает высокую культуру умственного труда, совершенствует способы организации познавательной деятельности, воспитывает ответственность, целеустремленность, систематичность и последовательность в работе студентов, развивает у них бережное отношение к своему времени, способность доводить до конца начатое дело.

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.2.

Для обеспечения самостоятельной работы обучающихся используются электронные курсы «Информационная безопасность» (<https://e-learning.unn.ru/enrol/index.php?id=4715> и <https://e-learning.unn.ru/enrol/index.php?id=4760>), созданные в системе электронного обучения ННГУ - <https://e-learning.unn.ru/>.

5. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю), включающий:

5.1. Описание шкал оценивания результатов обучения по дисциплине

Уровень сформированности компетенций (индикатора достижения компетенций)	Шкала оценивания сформированности компетенций						
	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	не зачтено		зачтено				
<u>Знания</u>	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибок.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Уровень знаний в объеме, превышающем программу подготовки
<u>Умения</u>	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продemonстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме.	Продemonстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения, решены все основные задачи с отдельными несущественным недочетами, выполнены все задания в полном объеме.	Продemonстрированы все основные умения, решены все основные задачи. Выполнены все задания, в полном объеме без недочетов

<u>Навыки</u>	Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач без ошибок и недочетов.	Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продemonстрирован творческий подход к решению нестандартных задач
---------------	--	--	---	---	---	---	---

Шкала оценки при промежуточной аттестации

Оценка		Уровень подготовки
	превосходно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне, выше предусмотренного программой
зачтено	отлично	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично»
	очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне «очень хорошо»
	хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «хорошо»
	удовлетворительно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
не зачтено	неудовлетворительно	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»
	плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения.

5.2.1 Контрольные вопросы к экзамену по дисциплине «Информационная безопасность»

Вопросы	Коды компетенции
Как построить программу безопасности	ОПК-6
Типы атак	ОПК-6
Лучшие практики сетевой защиты	ОПК-6
Использование для аутентификации	ОПК-6
Подходы к защите неструктурированных данных	ОПК-6
Установка и настройка клиента управления правами на информацию	ОПК-6

Современные коды шифрования	ОПК-6
Эволюция безопасности хранения	ОПК-6
Общие концепции безопасности баз данных	ОПК-6
Проектирование безопасности в сети	ОПК-6
Методы обеспечения безопасности коммутаторов	ОПК-6
Эволюция брандмауэров	ОПК-6
Беспроводное обнаружение и предотвращение вторжений	ОПК-6
Важность защиты информации	ПК – 3
Бизнес-процессы против технического контроля	ПК – 3
Анализ рисков	ПК – 3
Стандарты информационной безопасности	ПК – 3
Политика безопасности	ПК – 3
Планирование непрерывности бизнеса	ПК – 3
Соблюдение законов при реагировании на инциденты	ПК – 3
Реагирование на инциденты и судебно-медицинский анализ	ПК – 3
Оценка физической уязвимости	ПК – 3
Политика управления персоналом	ПК – 3

5.2.2. Типовые задания для оценки сформированности компетенции ОПК-6

Расшифруйте простую замену с известным кодом:

7 8 2 25 23 10 15 23 28 1 5 20 18 2 7 25 4 33 23 14 8 18 5 20 33 18 10 14 24 8 25 5 32 14 5 11
28 8 14 15 5 28 5 15 14 11 24 5 8 2 28 19 18 30 5 11 33 19 33 23 5 4 2 14 8 5 6 18 22 33 20 5 20 33
18 20 32 14 5 8 14 6 25 1 5 10 14 11 14 5 3 28 20 18 2 25 32 14 5 4 2 33 18 7 32 33 10 18 5 18 20 14
32 18 5 19 33 10 4 33 8 25 5 11 33 19 25 5 15 23 33 14 19 33 5 32 25 4 2 25 10 32 33 29 14 10 15 21
5 8 32 14 1 5 2 25 11 33 15 25 1 5 5 18 5 8 14 6 25 1 5 23 10 24 3 18 14 5 8 14 6 25 5 10 23 33 18 5
25 5 8 14 32 21 5 10 14 8 21 20 17 1 5 19 33 10 4 33 8 28 5 11 33 19 28 5 15 23 33 14 20 28 4 33 34
18 15 25 1 5 33 15 22 25 26 5 15 23 33 14 19 33 5 18 5 20 25 15 21 5 15 23 33 16 32 14 5 28 11 18 23
25 1 32 14 5 4 2 14 6 16 11 33 8 14 1 10 15 23 28 1 32 14 5 3 2 25 8 18 32 14 5 4 2 33 18 7 32 33 10
18 5 6 33 13 32 33 19 33 5 10 23 18 8 14 15 14 6 21 10 15 23 25 5 32 25 5 11 6 18 13 32 14 19 33 5
15 23 33 14 19 33 32 14 5 13 14 6 25 1 5 8 33 20 25 5 11 6 18 13 32 14 19 33 5 15 23 33 14 19 33 5
32 14 5 13 14 6 25 1 5 13 14 32 17 5 11 6 18 13 32 14 19 33 5 15 23 33 14 19 33 5 32 18 5 2 25 11 25
5 14 19 33 5 32 18 5 33 10 6 25 5 14 19 33 5 32 18 34 14 19 33 5 34 15 33 5 28 5 11 6 18 13 32 14 19
33 5 15 23 33 14 19 33 7 25 4 33 23 14 8 18 5 20 33 30 25 20 20 14 8 25 32 14 5 4 2 18 8 25 23 25 1 5
19 33 10 4 33 8 28 5 10 33 15 33 23 25 2 18 27 14 1 32 14 5 28 11 18 23 25 1 5 8 14 15 14 1 5 10 23
33 18 30 5 2 25 8 18 5 11 14 8 32 33 10 15 18 5 10 23 33 14 1 2 33 8 18 15 14 6 24 20 5 11 6 25 19 33
8 14 24 32 18 14 10 33 15 23 33 2 24 1 5 20 33 6 18 15 23 28 11 33 1 10 24 5 20 14 2 7 33 10 15 14 1

5.2.3 Типовые задания для оценки сформированности компетенции ПК-3

Найдите ключ простой подстановки на основе метода статистической частоты букв в русских текстах и расшифруйте текст:

10 32 25 30 11 16 12 26 11 4 12 26 10 22 24 10 14 4 18 20 30 25 30 26 10 13 15 6 13 8 32 10
14 20 24 26 13 26 8 32 16 29 18 16 21 26 11 30 4 8 16 30 26 28 21 14 31 26 23 16 30 25 30 26 23 13
8 32 10 14 20 24 26 26 32 10 4 18 26 8 18 1 16 31 26 18 1 4 18 7 16 32 26 11 32 4 30 20 24 12 26 19
13 16 33 34 18 12 26 10 4 24 28 32 32 14 26 15 30 4 30 20 24 12 26 26 33 26 6 30 11 18 16 32 26 4 2
28 30 20 31 26 13 26 16 24 10 26 20 26 18 1 28 21 14 33 32 26 14 32 15 4 18 14 10 12 26 13 26 33 24
8 11 30 25 30 26 20 26 25 6 13 11 18 26 4 13 22 7 32 26 23 21 26 15 6 30 15 31 32 23 26 32 32 26 11
30 26 16 18 14 33 18 26 16 30 26 20 6 24 25 13 26 20 26 30 28 18 11 13 26 16 32 26 11 24 11 18 23
26 26 11 32 16 31 26 33 30 14 30 6 21 27 26 15 4 30 3 30 26 16 24 22 24 14 26 16 32 26 28 6 24 16
18 26 14 30 10 33 4 18 20 30 26 16 30 12 26 15 30 14 30 23 13 26 22 14 30 26 18 26 13 11 24 22 24

26 13 14 6 30 23 28 26 10 15 18 14 26 30 14 26 15 32 6 32 15 30 12 26 26 23 16 32 26 8 24 4 31 26
 16 32 28 30 10 20 30 11 26 5 14 30 14 26 10 18 16 18 27 26 8 24 4 31 26 1 32 23 4 2 26 18 26 8 18 1
 16 18 26 30 10 33 30 4 33 18 26 23 16 32 26 10 14 6 24 7 16 30 26 22 14 30 26 10 21 14 21 32 26 10
 20 18 16 31 18 26 10 14 6 24 7 16 32 27 26 22 32 23 26 25 30 4 30 11 16 21 32 26 20 30 4 33 18 26
 26 30 25 6 30 23 32 16 26 11 30 4 25 26 16 24 7 26 6 24 1 16 21 23 26 4 2 11 12 23 26 24 26 28 4 18
 1 33 18 23 26 28 30 4 32 32 26 11 6 13 25 18 3 26 11 30 4 8 16 21 26 23 21 26 14 32 23 26 33 30 25
 30 26 23 21 26 4 2 28 18 23 26 13 8 32 26 1 24 26 14 30 26 22 14 30 26 4 2 28 18 23 26 18 3

6. Учебно-методическое и информационное обеспечение дисциплины

а) литература:

1. Mark Rhodes-Ousley. Information Security. New York, Chicago, San Francisco, Lisbon, London, Madrid, Mexico City, Milan, New Delhi, San Juan, Seoul, Singapore, Sydney, Toronto, 2013 – 898 p. – URL: [Information Security - The Complete Reference - PDF Drive](#)
2. Michael E. Whitman, Herbert J. Mattord. Principles of Information Security. Boston, 2017 – 750 p. – URL: [Principles of Information Security - PDF Drive](#)
3. Heru Susanto, Mohammad Nabil Almunawar. Information Security Management Systems. Oakville, 2018 – 327 p. – URL: [Information Security Management Systems : A Novel Framework and Software As a Tool for Compliance with Information Security Standard - PDF Drive](#)
4. Thomas Peltier. Information Security Policies, Procedures and Standards. Boca Raton, London, New York, Washington, D.C., 2001 – 314 p. – URL: [Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management by Thomas R. Peltier - PDF Drive](#)
5. Harold F. Tipton, Micki Krause Nozaki. Information Security Management Handbook. Boca Raton, 2012 – 494 p. – URL: [Information Security Management Handbook - PDF Drive](#)

б) программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины)

1. Dr. Soper. Information Security, Lessons 1-12. – URL: [Introduction to Computer Security - Information Security Lesson #1 of 12 - YouTube](#)
2. Операционная система Microsoft Windows
3. Прикладное программное обеспечение Microsoft Office

7. Материально-техническое обеспечение дисциплины

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения: компьютером, проектором или ЖК-телевизором, акустической системой и микрофоном (при необходимости), а также доской.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ОС ННГУ по направлению подготовки 38.03.01 Экономика (бакалавриат), профиль «Экономика, международный бизнес и предпринимательство».

Автор:

к.т.н., доцент

И.В. Носаков

Программа одобрена на заседании методической комиссии Института экономики и предпринимательства протокол № 0 от 00.00.0000 .