

Министерство сельского хозяйства Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Горский государственный аграрный университет»  
(ФГБОУ ВО Горский ГАУ)

Факультет экономики и менеджмента

Кафедра экономики и экономической безопасности

Учебный год 2023-2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННЫЕ РЕСУРСЫ В ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ  
ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ -  
ПРОГРАММА СПЕЦИАЛИТЕТА

Наименование направления подготовки	38.05.01 Экономическая безопасность
Направленность (профиль)	Экономико-правовое обеспечение экономической безопасности
Реквизиты федерального государственного образовательного стандарта высшего образования	Приказ Минобрнауки России от 14 апреля 2021 г. № 293
Год начала подготовки	2022
Очная форма обучения - учебные планы по годам приема	2023
Заочная форма обучения - учебные планы по годам приема	2022,2023
Номер по реестру ОП ВО ФГБОУ ВО Горский ГАУ	С-380501-2022 т
Реквизиты решения ученого совета ФГБОУ ВО Горский ГАУ об утверждении ОП ВО	Протокол от 11 апреля 2023 г. № 6
Реквизиты приказа ректора или уполномоченного лица об утверждении ОП ВО	Приказ врио ректора от 11 апреля 2023 г. № 85/06
Место дисциплины в структуре учебного плана	Часть, формируемая участниками образовательных отношений
Количество зачетных единиц	3

## 1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

№ №	Планируемые результаты освоения образовательной программы	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
	Код и наименование компетенции		
	ПК-1 Способность формировать, анализировать и оценивать информацию, необходимую для принятия решений по обеспечению экономической безопасности	ПК-1 И-1 Находит и формирует информационную базу, необходимую для обеспечения экономической безопасности	ПК-1. И-1. З-10. <i>Знает</i> принципы построения и использования информационных баз, методы и приемы анализа информации
			ПК-1. И-1. У-10. <i>Умеет</i> находить и формировать информационную базу, необходимую для обеспечения экономической безопасности
			ПК-1. И-1. В-10. <i>Владеет</i> методами анализа и оценки полученной информации, необходимой для нейтрализации угроз экономической безопасности
		ПК-1 И-2 Анализирует и оценивает полученную информацию, необходимую для нейтрализации угроз экономической безопасности	ПК-1. И-2. З-9. Знает методики расчета экономических показателей в соответствии с действующей нормативно-правовой базой
			ПК-1. И-2. У-9. Умеет рассчитывать экономические показатели, характеризующие социально-экономические процессы на различных уровнях
			ПК-1. И-1. В-9. Владеет навыками выбирать и обосновывать методики расчета экономических показателей в соответствии с действующей нормативно-правовой базой

## 2. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ

### 2.1. Трудоемкость дисциплины по видам учебной деятельности и формам обучения:

Виды учебной деятельности	Всего часов <u>108</u> , в том числе часов:	
	Очная форма обучения	Заочная форма обучения
Лекционные занятия	18	6
Практические занятия	24	8
Самостоятельная работа	66	94
Форма промежуточной аттестации	зачет	

### 2.2. Трудоемкость дисциплины по (разделам) темам:

№ № п/п	Наименование тем	Всего часов 108					
		Очная форма обучения			Заочная форма обучения		
		Лекции	Практические занятия	СРС	Лекции	Практические занятия	СРС
1	Теоретические аспекты информационной безопасности в экономических системах	2	2	6		2	10
2	Понятие информационных угроз и их виды	2	2	6			10
3	Нормативно-правовые основы информационной безопасности и защиты информации	2	2	6	2	2	10
4	Организация системы защиты информации экономических систем	4	2	8			10
5	Управление средствами обеспечения информационной безопасности экономической деятельности	4	2	8	2	2	10
6	Информационная безопасность как определяющий компонент национальной безопасности России	2	2	8			10
7	Угрозы информационной безопасности. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере	4	2	8			12
8	Общая характеристика способов и средств защиты информации	2	2	8	2	2	12

9	Основные направления обеспечения информационной безопасности компьютерных сетей учебных заведений	2	2	8			10
---	---	---	---	---	--	--	----

### 3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ

Тема 1. Теоретические аспекты информационной безопасности экономических систем. Основные понятия. Экономическая информация как товар и объект безопасности.

Цели и задачи дисциплины «Информационные ресурсы в деятельности по обеспечению экономической безопасности» это – защита экономических объектов и экономической среды от воздействия факторов риска в угрожающих ситуациях; проблема компьютерной преступности во всех странах мира, независимо от их географического положения, вызывает необходимость привлечения все большего внимания и сил общественности для организации борьбы.

Вопросы к практическому занятию:

1. Теоретические аспекты информационной безопасности экономических систем.
2. Основные понятия. Экономическая информация как товар и объект безопасности.

Вопросы для самостоятельной работы :

1. Юридические и организационные меры защиты

Тема 2. Понятие информационных угроз и их виды. Информационные угрозы. Вредоносные программы. Компьютерные преступления и наказания.

Вопросы к практическому занятию:

1. Информационные угрозы.
2. Вредоносные программы.
3. Компьютерные преступления и наказания.

Вопросы для самостоятельной работы:

1. Защита программ и ценных баз данных от несанкционированного копирования и распространения

Тема 3. Нормативно-правовые основы информационной безопасности и защиты информации.

Государственное регулирование информационной безопасности. Подходы, принципы, методы и средства обеспечения безопасности. Организационно-техническое обеспечение компьютерной безопасности. Защита от компьютерных вирусов. Электронная цифровая подпись и особенности ее применения.

Вопросы к практическому занятию:

1. Государственное регулирование информационной безопасности.
2. Подходы, принципы, методы и средства обеспечения безопасности.
3. Организационно-техническое обеспечение компьютерной безопасности.
4. Защита от компьютерных вирусов.
5. Электронная цифровая подпись и особенности ее применения.

Вопросы для самостоятельной работы:

1. Защита информации в Интернете.

Тема 4. Организация системы защиты информации экономических систем.

Этапы построения системы защиты информации. Политика безопасности. Оценка эффективности инвестиций в информационную безопасность.

Вопросы к практическому занятию:

1. Этапы построения системы защиты информации.
  2. Политика безопасности.
  3. Оценка эффективности инвестиций в информационную безопасность.
- Вопросы для самостоятельной работы:
1. Программно-аппаратные методы и средства защиты.

Тема 5. Управление средствами обеспечения информационной безопасности экономической деятельности.

Обеспечение информационной безопасности автоматизированных банковских систем. Информационная безопасность электронной коммерции. Обеспечение компьютерной безопасности учетной информации.

Вопросы к практическому занятию:

1. Обеспечение информационной безопасности автоматизированных банковских систем.
2. Информационная безопасность электронной коммерции.

Вопросы для самостоятельной работы:

3. Обеспечение компьютерной безопасности учетной информации.

Тема 6. Информационная безопасность как определяющий компонент национальной безопасности России.

Место информационной безопасности в системе национальной безопасности России: понятие, структура и содержание. Основные руководящие документы, регламентирующие вопросы информационной безопасности.

Вопросы к практическому занятию:

1. Место информационной безопасности в системе национальной безопасности России: понятие, структура и содержание.
2. Основные руководящие документы, регламентирующие вопросы информационной безопасности.

Вопросы для самостоятельной работы:

3. Современные угрозы информационной безопасности в России

Тема 7. Угрозы информационной безопасности. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере.

Информационные ресурсы и конфиденциальность информации. Угрозы конфиденциальной информации организации. Система защиты конфиденциальной информации.

Вопросы к практическому занятию:

1. Информационные ресурсы и конфиденциальность информации.
2. Угрозы конфиденциальной информации организации.
3. Система защиты конфиденциальной информации.

Вопросы для самостоятельной работы:

1. Понятие и виды защищаемой информации.

Тема 8. Общая характеристика способов и средств защиты информации.

Анализ и типизация организационных и программно-аппаратных структур автоматизированных систем предприятия. Анализ возможных угроз и их специфика в различных типах АС. Систематизация видов защиты информации.

Вопросы к практическому занятию:

1. Анализ и типизация организационных и программно-аппаратных структур автоматизированных систем предприятия.

2. Анализ возможных угроз и их специфика в различных типах АС.
3. Систематизация видов защиты информации.

Вопросы для самостоятельной работы:

1. Криптографические методы защиты информации.

Тема 9. Основные направления обеспечения информационной безопасности компьютерных сетей учебных заведений. Состояние вопросов обеспечения информационной безопасности. Угрозы и уязвимости КСУЗ. Этапы построения БКСУЗ.

Вопросы к практическому занятию:

1. Состояние вопросов обеспечения информационной безопасности.
2. Угрозы и уязвимости КСУЗ.
3. Этапы построения БКСУЗ.

Вопросы для самостоятельной работы:

1. Направление исследований.

#### 4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

##### 4.1. ОСНОВНАЯ ЛИТЕРАТУРА

1. Гусарова, И. А. Экономика предприятия : учебное пособие / И. А. Гусарова, Ю. В. Пантелеева, К. В. Николаева. — 2-е изд., перераб. и доп. — Казань : КНИТУ, 2022. — 100 с. — ISBN 978-5-7882-3196-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/330779>

2. Кислощаев, П. А. Экономическая безопасность: учебное пособие / П. А. Кислощаев, Н. В. Капитонова, С. В. Каминская ; под редакцией В. Ю. Бурова. — Чита : ЗабГУ, 2020. — 157 с. — ISBN 978-5-9293-2570-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/173697>

3. Лебедева, Е. С. Бухгалтерский учет в системе экономической безопасности предприятия : учебное пособие / Е. С. Лебедева. — Москва : РТУ МИРЭА, 2020. — 145 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/163902>

4. Мусаева, А. М. Экономическая безопасность секторов экономики : учебное пособие / А. М. Мусаева, Г. С. Султанов, М. К. Бамматханова. — Махачкала : ДагГАУ имени М.М.Джамбулатова, 2021. — 208 с. — ISBN 978-5-00128-799-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/254603>

5. Сергеев, А. Ю. Основы экономической безопасности : учебное пособие / А. Ю. Сергеев. — Пенза : ПГУ, 2019. — 212 с. — ISBN 978-5-907185-14-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/162294>

6. Управление экономической безопасностью : монография / под редакцией В. В. Красновой. — Донецк : ДонНУ, 2019. — 221 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/161977>

##### 4.2. ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

1. Асаул, А.Н.. Организация предпринимательской деятельности: учебник : Учебник / А.Н. Асаул — Санкт-Петербург : Архитектурно-строительный университет СПб, 2009. — 204 с. — ISBN 978-5-91460-023-2. — URL: <https://book.ru/book/908947>

2. Безопасность жизнедеятельности человека в окружающей среде : учебное пособие / составители В. И. Оберешин, Н. В. Минаева. — Рязань : РязГМУ, 2022. — 244 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/352394>

3. Саталкина, Н. И. Технологии антикризисного управления в экономической безопасности : учебное пособие / Н. И. Саталкина. — Тамбов : ТГТУ, 2021. — 100 с. — ISBN 978-5-8265-2444-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/320552>

4. Финансовые и учетно-аналитические проблемы устойчивого развития экономики : монография / Т. Н. Урядова, Е. А. Батищева, И. А. Демченко [и др.] ; под общей редакцией М. Г. Лещевой. — Ставрополь : СтГАУ, 2021. — 169 с. — ISBN 978-5-907110-92-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/245939>

#### 4.3. СОСТАВ ЛИЦЕНЗИОННОГО И СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, В ТОМ ЧИСЛЕ ОТЕЧЕСТВЕННОГО ПРОИЗВОДСТВА

1. Microsoft Windows 7 Pro
2. Office 2007 Standard
3. Moodle 3.8

#### 4.4. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ, ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ, ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ

1. Информационно-правовой портал «Гарант» <http://www.garant.ru/>
2. Система автоматизации библиотек ИРБИС64; ООО «ЭйВиДи –систем» <http://support.open4u.ru>
3. Электронная библиотечная система ООО «КноРус медиа» [www.book.ru](http://www.book.ru)
4. Электронная библиотечная система издательства «Лань». [www.e.lanbook.ru](http://www.e.lanbook.ru)
5. Национальная электронная библиотека (НЭБ). <http://нэб.рф>

#### 5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ УСЛОВИЯ, ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ

Для реализации дисциплины необходимы:

- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения: комплектом мебели для обучающихся, доской настенной, рабочим местом преподавателя, комплектом мультимедийного оборудования, экраном-доской;
- помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде университета;
- индивидуальный неограниченный доступ (в том числе удаленный) обучающихся к электронно - библиотечным системам и к электронной информационно-образовательной среде университета, к современным профессиональным базам данных и информационным справочным системам.

#### 6. ОЦЕНОЧНЫЕ СРЕДСТВА

6.1. Перечень вопросов к зачету:

1. Дайте определение понятия «информационная безопасность».
2. Дайте определение понятия «доступность информации». Поясните, что понимается под доступностью 15 компонента и ресурса.

3. Дайте определение понятия «целостность информации». Поясните, что понимается под целостностью компонента и ресурса.
4. Дайте определение понятия «конфиденциальность информации». Поясните, что понимается под правом и правилом доступа к информации.
5. Дайте определение понятия «объект информатизации».
6. Дайте определение понятия «информационные ресурсы (активы)».
7. Дайте определение понятий «собственник информации», «владелец информации», «пользователь информации».
8. Дайте определение понятия «защита информации».
9. Дайте определение понятия «объект защиты информации».
10. Дайте определение понятия «эффективность защиты информации». Поясните, в чем цель защиты информации.
11. Дайте определение понятий «санкционированный доступ к информации» и «несанкционированный доступ к информации».
12. Дайте определение понятий «идентификация субъекта» и «идентификатор».
13. Дайте определение понятий «аутентификация субъекта» и «авторизация субъекта».
14. Дайте определение понятий «защита информации от разглашения», «защищенная система», «средство защиты информации», «способ защиты информации», «комплекс средств защиты информации».
15. Дайте определение понятий «техника защиты информации» и «система защиты информации».
16. Раскройте суть фрагментарного подхода к решению проблемы обеспечения безопасности компьютерных систем и сетей.
17. Раскройте суть комплексного подхода к решению проблемы обеспечения безопасности компьютерных систем и сетей.
18. Опишите схему взаимодействия основных субъектов и объектов обеспечения информационной безопасности.
19. Охарактеризуйте отечественные и зарубежные источники информации и данных, необходимых для оценки информационной безопасности экономической деятельности организаций.
20. Раскройте систему мер защиты интересов субъектов информационных отношений.
21. Перечислите меры защиты информации законодательного уровня.
22. Перечислите меры защиты информации административно-организационного уровня.
23. Перечислите меры защиты информации программно-технического уровня.
24. Раскройте основные рекомендации ISTF по обеспечению информационной безопасности электронного бизнеса.
25. Раскройте систему нормативно-правовых актов в области информационной безопасности в РФ.
26. Охарактеризуйте предмет правового регулирования в сфере информационной безопасности.
27. Раскройте гарантии в сфере информации и информационной безопасности, закрепленные в нормах Конституции РФ.
28. Раскройте основные задачи обеспечения информационной безопасности, закрепленные в Концепции национальной безопасности РФ.
29. Перечислите подзаконные нормативные акты, регулирующие сферу информационной безопасности.
30. Дайте краткую характеристику положений ФЗ «Об информации, информационных технологиях и о защите информации».
31. Опишите, что вы понимаете под информацией, предоставляемой по соглашению лиц, участвующих в соответствующих отношениях. Приведите свои примеры такой информации.



32. Опишите, что вы понимаете под информацией, которая в соответствии с федеральными законами подлежит предоставлению или распространению. Приведите свои примеры такой информации.

33. Опишите, что вы понимаете под информацией, распространение которой в РФ ограничивается или запрещается. Приведите свои примеры такой информации.

34. Перечислите задачи защиты информации, определенные в ФЗ «Об информации, информационных технологиях и о защите информации».

35. Дайте краткую характеристику положений Федерального закона «О коммерческой тайне». 36. Дайте краткую характеристику положений Федерального закона «О персональных данных». 37. Дайте определение понятию «персональные данные»

## 6.2. Тестовые задания для диагностической работы.

1. Потенциальные убытки, которые понесет владелец информации, если к ней получат несанкционированный доступ сторонние лица – это

- а) стоимость утраты
- б) стоимость скрытого нарушения целостности
- в) стоимость потери конфиденциальности
- г) нет верного ответа

2. Ущерб полного или частичного разрушения информации – это

- а) стоимость утраты
- б) стоимость скрытого нарушения целостности
- в) стоимость потери конфиденциальности
- г) нет верного ответа

3. К конфиденциальным сведениям относят

- а) персональные данные граждан
- б) сведения, связанные с профессиональной деятельностью (врачебная, нотариальная, адвокатская тайны и пр.)
- в) сведения о сущности изобретения до момента официальной публикации о них
- г) сведения, полученные из внешних открытых источников
- д) сведения, полученные на веб-сайте компании
- е) сведения, подписанные руководством, для передачи вовне (конференции, презентации и пр.)

4. Не является преднамеренным воздействием на информационную систему

- а) подбор пароля
- б) хищение информации
- в) перехват информации
- г) модификация информации

5. Не является причиной случайных воздействий на информационную систему

- а) подбор пароля
- б) ошибки пользователей
- в) отказы и сбои аппаратуры
- г) помехи в линиях связи из-за воздействий внешней среды

6. Пути несанкционированной передачи информации

- а) негласный просмотр информации, отображенной на мониторе
- б) хищение носителей информации
- в) подключение к устройствам передачи, обработки и хранения информации
- г) внедрение резидентных программ
- д) установка прослушивающих и передающих устройств
- е) распространение информации ее владельцем

ж) регистрация и анализ побочных электромагнитных излучений компьютерной техники, средств связи и телекоммуникаций

7. Реализация угроз информационной безопасности может привести к

- а) уничтожению средств ввода-вывода информации
- б) несанкционированному доступу к информации
- в) изменению конфигурации периферийных устройств
- г) нет верного ответа

8. Результатом реализации угрозы перехвата может стать

- а) нарушение доступности данных
- б) отказ в обслуживании
- в) нарушение конфиденциальности данных
- г) изменение конфигурации периферийных устройств

9. При разработке модели нарушителя определяются такие предположения

- а) о категориях лиц, к которым может принадлежать нарушитель
- б) о мотивах действий нарушителя
- в) о квалификации нарушителя и его технической оснащенности
- г) о способности личности исполнять данную социальную роль
- д) о характере возможных действий нарушителя

10. Уголовно наказуемые общественно опасные действия, в которых машинная информация является объектом посягательства – это

- а) компьютерное преступление
- б) несанкционированное действие
- в) компьютерное мошенничество
- г) кража

11. Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, потере целостности, конфиденциальности, доступности информации – это

- а) угроза информационной безопасности
- б) фальсификация информации
- в) несанкционированный доступ к информации
- г) нет верного ответа

12. Комплекс средств и методов, направленных на предотвращение угроз информационной безопасности и устранение их последствий – это

- а) информационная безопасность
- б) компьютерная безопасность
- в) защита информации
- г) защита государственной тайны

13. Основными направлениями защиты информации являются

- а) предупреждение угроз
- б) выявление угроз
- в) ликвидация угроз
- г) ликвидация последствий угроз
- д) стабилизация угроз
- е) регистрация угроз

14. Действия, направленные на устранение действующей угрозы и конкретных преступных действий – это

- а) предупреждение угроз
- б) выявление угроз
- в) обнаружение угроз
- г) ликвидация угроз

15. Действия, направленные на преодоление конкретной угрозы и ее источников, приносящих тот или иной вид ущерба – это

- а) предупреждение угроз
- б) выявление угроз
- в) обнаружение угроз
- д) ликвидация угроз

16. Проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны криминальных структур или конкурентов на рынке – это

- а) предупреждение угроз
- б) выявление угроз
- в) обнаружение угроз
- г) ликвидация угроз

17. Реализация угроз информационной безопасности может привести к

- а) уничтожению средств ввода-вывода информации
- б) несанкционированному доступу к информации
- в) изменению конфигурации периферийных устройств
- г) нет верного ответа

18. Реализация угроз информационной безопасности может привести к

- а) уничтожению средств ввода-вывода информации
- б) несанкционированному доступу к информации
- в) изменению конфигурации периферийных устройств
- г) нет верного ответа

19. Результатом реализации угрозы перехвата может стать

- а) нарушение доступности данных
- б) отказ в обслуживании
- в) нарушение конфиденциальности данных
- г) изменение конфигурации периферийных устройств

20. Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб пользователям информации – это

- а) информационная безопасность
- б) компьютерная безопасность
- в) защита информации
- г) защита государственной тайны.