МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГАОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра информационной безопасности

СОЦИАЛЬНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность
Код и наименование направления подготовки/специальности

Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)
Наименование направленности (профиля)/ специализации

Уровень высшего образования:*бакалавриат*

Форма обучения:*очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2026

Социальные аспекты информационной безопасности
Рабочая программа дисциплины

Составитель(и):
Заведующий кафедрой ИБ
кандидат исторических наук, доцент Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры
Информационной безопасности
№ 5 от 10.12.2025

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: формирование культуры информационной безопасности (ИБ) в социальной среде.

Задачи дисциплины:

- изучение основных угроз ИБ в социальной среде;
- формирование знаний у обучающихся о правовых и организационных принципах обеспечения ИБ в социальной среде;
- выработка у обучающихся практических умений по использованию методов обеспечения ИБ.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-14 Способен организовывать работу малого коллектива исполнителей в профессиональной деятельности	ПК-14.1 Знает организацию проведения инструктажа руководящего состава и обучения персонала по вопросам защиты информации ПК-14.2 Умеет организовать работу персонала по использованию технических, программных (программно-технических) средств защиты информации ПК-14.3 Владеет навыками по осуществлению планирования и организации работы персонала с учетом требований по защите информации	Знать: основные принципы организации работы малого коллектива исполнителей в профессиональной деятельности; Уметь: организовывать работу малого коллектива исполнителей в профессиональной деятельности; Владеть: навыками использования нормативных документов, регламентирующих ИБ

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Социальные аспекты информационной безопасности» относится к части блока дисциплин, формируемых участниками образовательных отношений, учебного плана.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часов.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
7	Лекции	**28**
7	Практические занятия	**32**
	Всего:	**60**

Объем дисциплины в форме самостоятельной работы обучающихся составляет 48 академических часов.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1.	Государственная система защиты информации в России	Предмет и содержание дисциплины, методы изучения, основная литература, контроль освоения дисциплины. Структура государственной системы защиты информации в России. Основные объекты и субъекты защиты информации в России. Базовые уровни обеспечения информационной безопасности (ИБ). Основные угрозы ИБ. Основные механизмы защиты информации в информационных системах (ИС) и в информационно-телекоммуникационных сетях (ИТС).
2.	Социальный аспект исследования проблем защиты информации с учётом угроз информационной безопасности	Безопасность как высший интерес человечества. Базовые угрозы безопасности личности по Т. Гоббсу. Основные права государства для обеспечения безопасности граждан. Базовый методический подход к изучению проблем ИБ. Основные функции органов системы ИБ. Базовые структурные компоненты системы ИБ. Основные факторы, воздействующие на информационная безопасность как социальную систему. Социальный подход к защите информации как средство методологического анализа информационной безопасности
3.	Современные инновационные технологии: преимущества и социальные последствия	Основные факторы, способствующие в настоящее время повышению уязвимости информации в ИС и ИТС. Обзор компьютерных преступлений в России и в мире. Базовые инновационные технологии XXI века. Негативные аспекты, возникающие с развитием современных технологий и глобальных сетей и отрицательно влияющие на общество. Основные типы интернет-зависимости. Базовые интернет-риски для детей. Негативное влияние гаджетов на мышление человека. Основные симптомы социальной зависимости от соцсетей. Влияние отмены письма на этнос и личностные качества человека.
4.	Социальные сети как среда проведения тайных информационных операций	Информационная война в социальных сетях как особая форма ведения войны в киберпространстве Интернета. Иерархия человеческих потребностей по А. Маслоу. Основные типы ресурсов в формате Web 2.0. Базовые динамические характеристики, определяющие особенности функционирования социальных сетей. Возможности использования блогосферы в деструктивных целях. Особенности сетевого эффекта.

		Опыт США по использованию социальных сетей в целях осуществления «мягкого» перехвата власти. Цели создания методов и средств проведения информационных операций в сети Интернет. Особенности сети, образованной с использованием Интернет-ресурсов. Базовые компоненты сетевой социальной структуры. Основные ролевые типы участников социальной сети. Базовые классы деструктивных социальных сетей.
5.	Системный подход к противодействию информационного воздействия на социум	Основные направления реализации информационного суверенитета России. Базовые функции системы информационного противодействия. Система мероприятий по защите личности и социума от информационно-психологических операций. Способы срыва информационно-психологического воздействия противника на социальные системы. Базовые этапы ликвидации последствий информационно-психологических операций противника. Основные направления достижения эффективной информационной защиты социальных систем и силовых структур. Индикаторы манипулятивного информационного воздействия на служащих силовых структур.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебной работы	Информационные и образовательные технологии
1	2	3	4
1	*Государственная система защиты информации в России*	*Лекция 1* *Практическое занятие 1*	*Вводная лекция с использованием видеоматериалов* *опрос*
2	*Социальный аспект исследования проблем защиты информации с учётом угроз информационной безопасности*	*Лекция 2* *Практическое занятие 2*	*Лекция с использованием видеоматериалов* *опрос*
3	*Современные инновационные технологии: преимущества и социальные последствия*	*Лекция 3* *Практическое занятие 3*	*Лекция с использованием видеоматериалов* *опрос*
4	*Социальные сети как среда проведения тайных информационных операций*	*Лекция 4* *Практическое занятие*	*Лекция с использованием видеоматериалов* *опрос*
5	*Системный подход к противодействию информационного воздействия на социум*	*Лекция 5* *Контрольная работа*	*Лекция с использованием видеоматериалов* *Подготовка к контрольной с использованием материалов лекций и литературы*

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля		**Макс. количество баллов**	
За одну работу	**Всего**		
Текущий контроль:			
- *опрос*		10 баллов	40 баллов
- *контрольная работа*		20 баллов	20 баллов
Промежуточная аттестация – *зачет* (*тестирование*)			40 баллов
Итого за семестр			100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично/ зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо/ зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно/ зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет-ворительно/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Примерные контрольные вопросы по курсу

1. Основные источники угроз информационной безопасности.
2. Базовые негативные аспекты, возникающие с развитием современных ИТ и глобальных сетей.
3. Модели распространения информации в блогосфере.
4. Базовые динамические характеристики, определяющие особенности функционирования социальных сетей.
5. Классификация программ США по созданию средств глобального контроля и использования Интернет для информационного превосходства над странами.
6. Характерные черты «цветных» революций.
7. Основные задачи систем мониторинга и анализа социальных сетей.
8. Ролевые типы участников социальной сети.
9. Основные возможности использования блогосферы в деструктивных целях.
10. Базовые задачи систем мониторинга и анализа социальных сетей.
11. Основные направления НИОКР, проводимых США в целях достижения информационного превосходства.
12. Особенности прогнозирования информационно-психологических операций.
13. Содержание комплекса мероприятий по нейтрализации психологических операций.
14. Основные элементы системы мероприятий по защите социума от информационно-психологических операций.
15. Стратегические цели обеспечения в РФ национальной безопасности в сфере культуры.
16. Основные направления достижения эффективной информационной защиты социальных систем.
17. Этапы разработки возможного воздействии на социальную сеть в рамках модели «цветных» революций.

18. Базовые индикаторы манипулятивного информационного воздействия на служащих силовых структур со стороны средств массовой информации.

19. Основные приоритеты в России в области обеспечения ИБ.

20. Базовые приоритеты информационной политики России в культурноинформационной сфере.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

Основные

1. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006, № 149-ФЗ // СЗ РФ 31.07.2006, № 31 (1 ч.). - Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_61798/

2. Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы (утверждена Указом Президента Российской Федерации от 9 мая 2017 г., № 203). - Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_216363/

Литература

Основная:

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 5-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2026. — 384 с. — (Высшее образование). — DOI: https://doi.org/10.29039/02005-0. - ISBN 978-5-369-02005-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2233509. – Режим доступа: по подписке.

2. Драгунова, Е. В. Основы цифрового общества : учебное пособие / Е. В. Драгунова. — Новосибирск : НГТУ, 2024. — 120 с. — ISBN 978-5-7782-5168-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/514391 (дата обращения: 27.02.2026). — Режим доступа: для авториз. пользователей.

3. Гафнер В.В. Информационная безопасность (учебное пособие). Ростов на Дону: «ФЕНИКС», 2010. - 330 с. - Режим доступа: - URL: https://elibrary.ru/download/elibrary_21292804_58225533.pdf

4. Редькина, Н. С. Основы информационной культуры и информационной безопасности : учебное пособие / Н.С. Редькина. — Москва : ИНФРА-М, 2025. — 193 с. — (Среднее профессиональное образование). - ISBN 978-5-16-020142-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2161237– Режим доступа: по подписке.

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:

1. Консультант Плюс

2. Гарант

7. . Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые доской, компьютером или ноутбуком, проектором (стационарным или переносным) для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.

• для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

• для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;

• для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;

• для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических занятий

Тема 1. Комплексный подход к формированию системы "информационная безопасность"- (2 часа)

Вопросы для изучения и обсуждения:

1. Основные компоненты системного подхода к формированию системы "информационная безопасность".
2. Система основных факторов ИБ.
3. Угрозы ИБ как главные структурные компоненты системы ИБ.
4. Базовые структурные компоненты системы "информационная безопасность".

Контрольные вопросы:

1. Основные функции системы "информационная безопасность".
2. Базовые подсистемы системы "информационная безопасность".
3. Основные факторы, способствующие повышению уязвимости информации.
4. Постройте иерархическую систему из понятий: информационная безопасность, защита данных, информация, компьютерная безопасность.

Тема 2. Социальные последствия реализации современных технологий, методов и средств защиты информации - (2 часа)

Вопросы для изучения и обсуждения:

1. Негативные аспекты, возникающие с развитием современных ИТ и глобальных сетей и отрицательно влияющие на общество.
2. Базовые симптомы социальной зависимости от социальных сетей.
3. Основные типы интернет-зависимости.
4. Охарактеризуйте тип мышления, формирующийся у активных участников социальных сетей.

Контрольные вопросы:

1. Базовые интернет-риски для детей.
2. Основные виды несанкционированного доступа к информационным системам, информационно-телекоммуникационным сетям и их влияние на субъектов информационных отношений.
3. Охарактеризуйте динамику финансового ущерба в мире от компьютерных преступлений.
4. Современная роль телевидения и его влияние на общество.

Тема 3. Социальные сети как платформа для организации и отражения социальных взаимоотношений - (2 часа)

Вопросы для изучения и обсуждения:

1. Базовые динамические характеристики, определяющие особенности функционирования социальных сетей.

2. Основные типы ресурсов в формате Web 2.0.

3. Опыт США по использованию социальных сетей с целью осуществления «мягкого» перехвата власти.

4. Особенности сетевого эффекта.

Контрольные вопросы:

1. Возможности использования блогосферы в деструктивных целях.

2. Основные ролевые типы участников социальной сети.

3. Цели создания методов и средств проведения информационных операций в сети Интернет.

4. Базовые классы деструктивных социальных сетей.

Тема 4. Система информационного противодействия по организации и ведению информационного противоборства - (2 часа)

Вопросы для изучения и обсуждения:

1. Основные направления реализации информационного суверенитета России.

2. Система мероприятий по защите личности и социума от информационно-психологических операций.

3. Основные функции системы информационного противодействия.

4. Способы срыва информационно-психологического воздействия противника на социальные системы.

Контрольные вопросы:

1. Состав мероприятий по защите социума от информационно-психологических операций противника.

2. Основные меры, предпринимаемые для ликвидации последствий информационно-психологических операций противника.

3. Базовые приоритеты России в области обеспечения ИБ.

4. Основные направления НИОКР, проводимых США в целях достижения информационного превосходства.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Цель дисциплины - формирование культуры информационной безопасности (ИБ) в социальной среде.

Задачи дисциплины:

- изучение основных угроз ИБ в социальной среде;
- формирование знаний у обучающихся о правовых и организационных принципах обеспечения ИБ в социальной среде;
- выработка у обучающихся практических умений по использованию методов обеспечения ИБ.

В результате освоения дисциплины (модуля) обучающийся должен:

Знать: организацию проведения инструктажа руководящего состава и обучения персонала по вопросам защиты информации

Уметь: организовать работу персонала по использованию технических, программных (программно-технических) средств защиты информации

Владеть: навыками по осуществлению планирования и организации работы персонала с учетом требований по защите информации