МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Факультет социальных наук
(факультет / институт / филиал)

УТВЕРЖДЕНО
Ученым советом ННГУ,
16 июня 2021 года, протокол № 8

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(наименование дисциплины (модуля))

Уровень высшего образования
бакалавриат
(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность
39.03.01 Социология
(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы
Социальная теория и комплексный анализ данных
(указывается профиль / магистерская программа / специализация)

Форма обучения
очная
(очная / очно-заочная / заочная)

Нижний Новгород
2021

Лист актуализации

Визирование РПД для исполнения в очередном учебном году

Председатель МК
__ _____ 2019 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2019-2020 учебном году на заседании кафедры
_____

Протокол от __ _____ 20___ г. № __
Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Председатель МК
__ _____ 20__ г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2020-2021 учебном году на заседании кафедры
_____

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Председатель МК
__ _____ 2021_ г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2021-2022 учебном году на заседании кафедры
_____

Протокол от __ _____ 20___ г. № __
Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Председатель МК
__ _____ 20___ г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры
_____

Протокол от __ _____ 20___ г. № __
Зав. кафедрой _____

1. Место дисциплины (модуля) в структуре ООП

Дисциплина *Информационная безопасность* относится к части ООП формируемой участниками образовательных отношений по направлению подготовки 39.03.01 «Социология». Дисциплина преподается в 8 семестре.

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****	
УК-8 Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуации	УК-8.1. Анализирует факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений)	*Знать* методологические основания социологического исследования *Уметь* производить, отбирать, обрабатывать и анализировать данные о социальных процессах и социальных общностях *Владеть* применением в соответствии с целями конкретного исследования методами сбора и анализа данных, учитывая их ограничения, и оценивая качество (валидность и надежность) социологической информации	*Работа на семинарах*
	УК-8.2. Идентифицирует опасные и вредные факторы в рамках осуществляемой деятельности	*Знать* основные закономерности развития комплексных социальных процессов *Уметь* использовать современные технологии для анализа социологических данных, создания баз данных, в том числе с помощью пакетов статистических программ *Владеть 2:* Принципами анализа и прогнозирования социальных явлений	*Работа на семинарах*
	УК-8.3. Выявляет проблемы, связанные с нарушениями техники безопасности на рабочем месте; предлагает мероприятиях по предотвращению чрезвычайных ситуаций	*Знать* специфику аналитической и экспертной деятельности *Уметь* участвовать в проектных формах работы и реализовывать самостоятельные проекты *Владеть* навыками использования информационных технологий при анализе социологических данных	*Работа на семинарах*

3. Структура и содержание дисциплины

3.1. Трудоемкость дисциплины

	очная форма обучения
Общая трудоемкость	3 ЗЕТ
Часов по учебному плану	108
в том числе	
аудиторные занятия (контактная работа): - занятия лекционного типа - занятия семинарского типа	22 10 10
самостоятельная работа	50
Промежуточная аттестация	*экзамен*

3.2. Содержание дисциплины

Наименование и краткое содержание разделов и тем дисциплины, форма промежуточной аттестации по дисциплине	Всего (часы)	В том числе:					
		Контактная работа (работа во взаимодействии с преподавателем), часы из них					Самостоятельная работа обучающегося, часы
		Занятия лекционного типа	Занятия семинарского типа	Занятия лабораторного типа	Консультации	Всего	
1. Введение в информационную безопасность	6	1	1				4
2. Правовое обеспечение информационной безопасности	6	1	1				4
3. Организационное обеспечение информационной безопасности	6	1	1				4
4. Технические средства и методы защиты информации	6	1	1				4
5. Программно-аппаратные средства и методы обеспечения информационной безопасности	6	1	1				4
6. Криптографические методы защиты информации	10	1	1		2		6
7. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	8	1	1				6
8. Использование криптографических средств защиты информации	8	1	1				6
9. Реализация работы инфраструктуры открытых ключей	8	1	1				6
10. Средства стеганографии для защиты информации	8	1	1				6
Промежуточная аттестация 36 часов (экзамен)							
Итого	108	10	10	-	2	24	50

Текущий контроль успеваемости реализуется в рамках занятий семинарского типа.

Промежуточная аттестация проходит в форме *экзамена*.

Занятия семинарского типа (практические 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 предусматривает:

– обсуждение практических вопросов на занятии,

– выполнение самостоятельной работы с анализом конкретной ситуации (кейса) с решением прикладной задачи.

На проведение практических занятий в форме практической подготовки отводится 8 часов.
Практическая подготовка направлена на формирование и развитие:
- практических навыков в соответствии с профилем образовательной программы: экспертно-диагностических и научно-исследовательских;
- компетенций (п.1 данной РПД).
Текущий контроль успеваемости реализуется в рамках занятий семинарского типа.

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

В ходе выполнения самостоятельной работы по данной дисциплине студенты выполняют по каждой теме следующий ряд работ:

- повторение конспекта лекций;
- работа над основной и дополнительной литературой (п. 5.1);
- выполнение заданий для самостоятельной работы (п. 5.2).

Учебно-методическим обеспечением самостоятельной работы являются все источники основной и дополнительной литературы, Интернет-ресурсов.

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

Уровень сформированности компетенций (индикатора достижения компетенций)	**Шкала оценивания сформированности компетенций**						
	плохо	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**очень хорошо**	**отлично**	**превосходно**
	Не зачтено		**Зачтено**				
Знания	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 ошибки	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
Умения	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения. Решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
Навыки	Отсутствие владения материалом. Невозможность оценить наличие навыков	При решении стандартных задач не продемонстрированы базовые	Имеется минимальный набор навыков для решения стандартных задач с некоторыми	Продемонстрированы базовые навыки при решении стандартных задач с	Продемонстрированы базовые навыки при решении стандартных задач без	Продемонстрированы навыки при решении нестандартных задач без ошибок и	Продемонстрирован творческий подход к решению нестандартных задач

	вследствие отказа обучающегося от ответа	навыки. Имели место грубые ошибки	недочетами	некоторыми недочетами	ошибок и недочетов	недочетов	

Шкала оценки при промежуточной аттестации

Оценка		Уровень подготовки
Зачтено	Превосходно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно»
	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

Контрольные вопросы для самостоятельной оценки качества освоения учебной дисциплины:

5.2.1. Контрольные вопросы

Вопрос	*Код компетенции*
1. Цели государства в области обеспечения информационной безопасности.	УК-8
2. Основные нормативные акты РФ, связанные с правовой защитой информации.	УК-8
3. Виды компьютерных преступлений.	УК-8
4. Способы и механизмы совершения информационных компьютерных преступлений.	УК-8
5. Основные параметры и черты информационной компьютерной преступности в России.	УК-8
6. Компьютерный вирус. Основные виды компьютерных вирусов.	УК-8
7. Методы защиты от компьютерных вирусов.	УК-8
8. Типы антивирусных программ.	УК-8
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.	УК-8
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.	УК-8
11. Виды защищаемой информации.	УК-8

12. Государственная тайна как особый вид защищаемой информации.	УК-8
13. Конфиденциальная информация.	УК-8
14. Система защиты государственной тайны.	УК-8
15. Правовой режим защиты государственной тайны.	УК-8
16. Защита интеллектуальной собственности средствами патентного и авторского права.	УК-8
17. Международное законодательство в области защиты информации.	УК-8
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.	УК-8
19. Симметричные шифры.	УК-8
20. Ассиметричные шифры.	УК-8
21. Криптографические протоколы.	УК-8
22. Криптографические хеш-функции.	УК-8
23. Электронная подпись.	УК-8
24. Организационное обеспечение информационной безопасности.	УК-8

5.2.2. Типовые задания/задачи для оценки сформированности компетенций УК-8

Тема 1. Введение в информационную безопасность

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Что такое правовые методы защиты информации?
6. Что такое организационные методы защиты информации?
7. Что такое технические методы защиты информации?
8. Что такое программно-аппаратные методы защиты информации?
9. Что такое криптографические методы защиты информации?
10. Что такое физические методы защиты информации?
11. Какие главные государственные органы в области обеспечения информационной безопасности?
12. Перечислите виды защищаемой информации.

Тема 2. Правовое обеспечение информационной безопасности

1. Какие основные законы в области защиты информации в РФ?
2. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
3. Что такое концепция информационной безопасности?
4. Что такое конфиденциальная информация?
5. Что такое персональные данные?
6. В каких случаях возможно использовать персональные данные без согласия обладателя?
7. Охарактеризуйте биометрические данные как персональные данные.
8. Что такое профессиональная тайна?
9. Что такое коммерческая тайна?
10. Что такое режим коммерческой тайны?
11. Что такое государственная тайна?
12. Опишите правовой режим государственной тайны.
13. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?

Тема 3. Организационное обеспечение информационной безопасности

1. Какие основные международные стандарты в области информационной безопасности существуют?
2. Что такое "Единые критерии"
3. Как связаны международные стандарты и стандарты РФ?
4. Какие основные стандарты РФ в области информационной безопасности существуют?
5. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.
6. Что такое политика безопасности?
7. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?

Тема 4. Технические средства и методы защиты информации

1. Что такое инженерная защита объектов?
2. Какие виды сигнализаций устанавливаются для обеспечения инженерной защиты?
3. Что такое технические каналы утечки информации?

4. Перечислите основные виды технических каналов утечки информации?
5. Перечислите методы защиты информации от утечки по визуальному каналу.
6. Перечислите методы защиты информации от утечки по воздушному каналу.
7. Перечислите методы защиты информации от утечки по вибрационному каналу.
8. Перечислите методы защиты информации от утечки по индукционному каналу.
9. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
10. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.

Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности

1. Какие виды компьютерных угроз существуют?
2. Что такое брандмауэр?
3. Что такое антивирусная программа?
4. Что такое эвристический алгоритм поиска вирусов?
5. Что такое сигнатурный поиск вирусов?
6. Методы противодействия сниффингу?
7. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
8. Что такое механизм контроля и разграничения доступа?
9. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
10. Что такое средства стеганографической защиты информации?

Тема 6. Криптографические методы защиты информации

1. Что такое криптография?
2. Какие используются симметричные алгоритмы шифрования?
3. Какие используются ассиметричные алгоритмы шифрования?
4. Что такое криптографическая хеш-функция?
5. Какие используются криптографические хеш-функции?
6. Что такое цифровая подпись?
7. Что такое инфраструктура открытых ключей?
8. Какие российские и международные стандарты на формирование цифровой подписи существуют?
9. Какие основные криптографические протоколы используются в сетях?

6. Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература

1. Информационная безопасность открытых систем [Электронный ресурс] / Мельников Д.А. М.: ФЛИНТА, 2014. http://www.studentlibrary.ru/book/ISBN9785976516137.html
2. Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф. М.: ДМК Пресс, 2014. http://www.studentlibrary.ru/book/ISBN9785940747680.html
3. Информационная безопасность: защита и нападение [Электронный ресурс] / Бирюков А.А. М.: ДМК Пресс, 2012. http://www.studentlibrary.ru/book/ISBN9785940746478.html
4. Безопасность информационных систем [Электронный ресурс] / Ерохин В.В. - М.: ФЛИНТА, 2015. - http://www.studentlibrary.ru/book/ISBN9785976519046.html

б) Дополнительная литература

1. Безопасность информации в автоматизированных системах [Электронный ресурс] / В.В. Мельников. - М.: Финансы и статистика, 2003. - http://www.studentlibrary.ru/book/ISBN5279025607.html

2. Глобальное управление Интернетом и безопасность в сфере использования ИКТ: Ключевые вызовы для мирового сообщества [Электронный ресурс] / Демидов О. - М.: Альпина Паблишер, 2016. - http://www.studentlibrary.ru/book/ISBN9785961458206.html

3. Безопасность систем баз данных [Электронный ресурс]: учеб. пособие / Скрыпников А.В., Родин С.В., Перминов Г.В., Чернышова Е.В. - Воронеж : ВГУИТ, 2015. - http://www.studentlibrary.ru/book/ISBN9785000321225.html

4. Бизнес-безопасность [Электронный ресурс] / И.Н. Кузнецов. - 4-е изд. - М.: Дашков и К, 2016. - http://www.studentlibrary.ru/book/ISBN9785394026546.html

в) Программное обеспечение и интернет-ресурсы:

Интернет-ресурсы:
http://www.lib.unn.ru/ - фундаментальная библиотека ННГУ
http://www.mid.ru – Министерство иностранных дел
http://www.fsb.ru/ - Федеральная служба безопасности

7. Материально-техническое обеспечение дисциплины

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения.

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 с учетом рекомендаций и ООП ВО направления подготовки 39.03.01 Социология (Социальная теория и комплексный анализ данных).

Автор
доцент кафедры социальной безопасности
и гуманитарных технологий, к.и.н. _____ Голубин Р.В.