Федеральное государственное бюджетное образовательное учреждения
высшего образования
Московский государственный университет имени М.В. Ломоносова
Социологический факультет

УТВЕРЖДАЮ
Декан социологического факультета,
профессор
_____/Н.Г. Осипова/
« » _____ 2023 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
# ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## BASIS OF INFORMATION SECURITY

Уровень высшего образования:
**Бакалавриат**

**Направление подготовки (специальность):**
41.03.06 - Публичная политика и социальные науки

Направленность (профиль) ОПОП:
**Экспертная деятельность в управлении социально-политическими проектами**

Форма обучения:
очная

Рабочая программа рассмотрена и одобрена
На заседании Ученого Совета факультета
(протокол №__ от_____ 2023 г.)

Москва 2023

Рабочая программа дисциплины (модуля) разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 41.03.06 – Публичная политика и социальные науки (уровень бакалавриата), утверждённым приказом Министерства образования и науки РФ № 1001 от 13 августа 2020 г. (с изменениями и дополнениями от 26.11.2020г.)

Год (годы) приёма на обучение: 2021, 2022, 2023

**1. Место дисциплины (модуля) в структуре ОПОП ВО**: относится к профессиональному циклу базовой части, 7 семестр.

**2. Входные требования для освоения дисциплины (модуля),** предварительные условия: в освоении дисциплины «Основы информационной безопасности» студенты опираются на знания, которые они получили в ходе изучения гуманитарных, социально-политических и естественнонаучных дисциплин, а также тех дисциплин, в которых изучаются методы осуществления информационной безопасности.

**3. Результаты обучения по дисциплине (модулю),** соотнесённые с требуемыми компетенциями выпускников.

| **Компетенции выпускников (коды)** | **Индикаторы (показатели) достижения компетенций** | **Планируемые результаты обучения по дисциплине (модулю), сопряжённые с компетенциями** |
|---|---|---|
| ОПК-2 Способен применять информационно-коммуникационные технологии и программные средства для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры и требований информационной безопасности | ОПК-2.1.<br>Использует информационно-коммуникационные технологии и программные средства для поиска, обработки информации по поставленной проблематике на основе принятых профессиональных норм и с учетом требований информационной безопасности | **Знать** основы информационной безопасности.<br>**Знать** информационно-коммуникационные технологии<br>**Уметь** обоснованно отбирать ИКТ для поиска, обработки информации по поставленной проблематике<br>**Владеть** основами информационно-библиографической культуры |

**4. Формат обучения:** очный.

**5. Объём дисциплины (модуля)** составляет 2 з.е., в том числе 36 академических часа, отведенных на контактную работу обучающихся с преподавателем, 36 академических часов на самостоятельную работу обучающихся.

**6. Содержание дисциплины (модуля),** структурированное по темам (разделам) с указанием отведённого на них количества академических часов и виды учебных занятий:

| **№ п/п** | **Наименование разделов и тем дисциплин /** | **Трудоёмкость (в ак. часах) по формам занятий (для дисциплин) и видам работ (для практик)** | | | **Формы контроля самостоятельной работы** |
|---|---|---|---|---|---|
| | | **Контактная работа** | | **ВСЕГО** | |

| | **Наименование разделов (этапов) практики** | **(работа во взаимодействии с преподавателем)** ***Виды контактной работы, часы*** | | | ***Самостоятельная работа*** | | |
|---|---|---|---|---|---|---|---|
| | | ***Лекции*** | ***Практические занятия (семинары)*** | ***всего*** | | | |
| 1 | **Тема 1.** Введение в информационную безопасность. | 2 | | 2 | 2 | 4 | Тема1. Контрольные вопросы и задания для самостоятельной работы. Дискуссия. Эссе. |
| 2 | **Тема 2.** Обеспечение информационной безопасности общества как основа государственной информационной политики. | 4 | | 4 | 4 | 8 | Тема 2. Контрольные вопросы и задания для самостоятельной работы Дискуссия. Эссе. |
| 3 | **Тема 3.** Информационная безопасность как предмет философско-политологического осмысления. | 2 | | 2 | 2 | 4 | Тема 3. Контрольные вопросы и задания для самостоятельной работы Дискуссия. Эссе. |
| 4 | **Тема 4.** Информационная война: сущность, разновидности, средства и методы ведения. | 2 | | 2 | 2 | 4 | Тема 4. Контрольные вопросы и задания для самостоятельной работы Дискуссия. Эссе. |
| 5 | **Тема 5.** Информационная безопасность политического пространства. | 2 | | 2 | 2 | 4 | Тема 5. Контрольные вопросы и задания для самостоятельной работы Дискуссия. Эссе. |
| 6 | **Тема 6.** Информационная ответственность субъектов политических отношений. | 2 | | 2 | 2 | 4 | Тема 6. Контрольные вопросы и задания для самостоятельной работы Дискуссия. Эссе. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | **Тема 7.** Экономика информационной безопасности. | 2 | | 2 | 2 | 4 | Тема 7. Контрольные вопросы и задания для самостоятельной работы Дискуссия. Эссе. |
| 8 | **Тема 8.** Технические средства защиты информации | 4 | | 4 | 4 | 8 | Тема 8. Контрольные вопросы и задания для самостоятельной работы Дискуссия. Эссе. |
| 9 | **Тема 9.** Средства защиты информации в автоматизированных информационных системах | 4 | | 4 | 4 | 8 | Тема 9. Контрольные вопросы и задания для самостоятельной работы Дискуссия. Эссе. |
| 10 | **Тема 10.** Основы защиты данных персонального компьютера | 4 | | 4 | 4 | 8 | Тема 10. Контрольные вопросы и задания для самостоятельной работы Дискуссия. Эссе. |
| 11 | **Тема 11.** Основы безопасности в Интернете | 4 | | 4 | 4 | 8 | Тема 11. Контрольные вопросы и задания для самостоятельной работы Дискуссия. Эссе. |
| 12 | **Тема 12.** Методология построения защищенных автоматизированных информационных систем | 4 | | 4 | 4 | 8 | Тема 12. Контрольные вопросы и задания для самостоятельной работы Дискуссия. Эссе. |
| | | **Промежуточный контроль (зачет)** | | | | | |
| **13** | **Итого: 72** | **36** | | **36** | **36** | **72** | |

**Содержание учебной дисциплины**

**Тема 1. Введение в информационную безопасность**

Назначение, задачи и общая характеристика курса, общие понятия и определения, краткая историческая справка. Данные и информация. Свойства информации. Представление информации и процессы ее обработки. Виды и формы представления информации. Носители информации. Информация как объект защиты. Определение и цели, механизмы, инструментарий, основные направления информационной

безопасности. Информация и ресурсы. Информация как объект права собственности. Информация как коммерческая тайна. Информация как рыночный продукт.

**Тема 2. Обеспечение информационной безопасности общества как основа государственной информационной политики**

Государственная информационная политика, ее определение, сущность. Особенности государственной информационной политики в современной России. «Доктрина информационной безопасности Российской Федерации».

Функциональные различия типов массово-информационной деятельности. Информационная агрессия и способы ее нейтрализации.

Понятие системы защиты информации. Виды обеспечения защиты информации. Служба информационной безопасности. Критерии необходимости создания. Основные понятия, задачи, функции, структура, принципы и этапы создания. Уровень подготовки специалистов. Подбор кадров. Взаимодействие с другими подразделениями организации. Оценка эффективности службы информационной безопасности.

**Тема 3. Информационная безопасность как предмет философско-политологического осмысления**

Определения понятия «безопасность» представителей разных философских школ. Динамика развития понятийного аппарата «безопасность». Информационная безопасность, ее специфика. Определение информационной безопасности.

Объекты обработки и защиты информации. Классификация информационных систем и объектов, модель классификации. Классификация средств обработки информации: стандарт CCITSE. Требования к функциональности безопасности. Требования к достоверности безопасности. Проверка соответствия информации средствам работы с ней.

**Тема 4. Информационная война: сущность, разновидности, средства и методы ведения**

Понятия «информационная война», «информационное оружие». Разновидности информационной войны. «Стратегическое информационное противоборство первого поколения» и «Стратегическое информационное противоборство второго поколения», их сущность и различия. Технологии манипулятивного воздействия. «Пятая колонна», ее значение при ведении информационной войны.

Понятие угрозы. Естественные и искусственные, случайные и преднамеренные, пассивные и активные, внешние и внутренние и т.п. угрозы. Источники угроз. Виды угроз: нарушение конфиденциальности, нарушение целостности, нарушение уровня доступности. Виды противников или "нарушителей". Модель нарушителя (злоумышленника).

Типовые модели нападения. Классификация атак. Типовая атака: снаружи и внутри. Локальные атаки. Удаленные атаки. Атаки на поток данных: пассивные и активные.

**Тема 5. Информационная безопасность политического пространства**

Понятие политического пространства, различные подходы к его изучению. Трансформация политического пространства в информационное пространство политики. Границы информационного пространства политики. Субъекты информационного пространства политики, их способы взаимодействия, инструменты реализации интересов. Принципы и технологии обеспечения информационной безопасности, применяемые в разных странах мира.

**Тема 6. Информационная ответственность субъектов политических отношений**

Субъекты политики с точки зрения традиционной политологии. Особенности и значение СМИ как субъекта политики на современном этапе развития общества. Трансформация роли традиционных политических институтов. Информационное пространство, порождаемое субъектом политики.

**Тема 7. Экономика информационной безопасности**

Идентификация рисков. Объективные и субъективные вероятности реализации угроз посредством уязвимостей и их оценка. Измерение рисков, шкалы рисков. Формирование качественных и количественных оценок рисков. Оценки потерь. Технологии оценки угроз, уязвимостей, рисков и потерь. Оптимизация потерь, обоснование прогноза потерь и ущерба. Методика выбора компонентов системы защиты информации и предполагаемая оценка ее эффективности. Экономические проблемы информационных ресурсов; экономическая безопасность; информация как важнейший ресурс экономики; информация как товар, цена информации; основные подходы к определению затрат на защиту информации; система ресурсообеспечения защиты
информации и эффективность ее использования; управление ресурсами в процессе защиты информации; виды ущерба, наносимые информации; степень наносимого ущерба информации; методы и способы страхования информации; формирование бюджета службы защиты информации; оценка эффективности защиты и страхования информации.

**Тема 8. Технические средства защиты информации**

Устройства и системы противоправного преднамеренного овладения конфиденциальной информацией. Технические средства защиты объектов. Инженерно-техническая защита. Системы охранной сигнализации на территории и в помещениях объекта обработки информации. Требования к системам охранной сигнализации. Наружные системы охраны. Традиционные системы. Ультразвуковые системы. Системы прерывания луча. Телевизионные системы. Радиолокационные системы. Микроволновые системы. Беспроводные системы. Система охранной (пожарной) сигнализации. Система хранения. Интеграция систем контроля. Система контроля вскрытия аппаратуры. Требования, предъявляемые к системе контроля вскрытия аппаратуры. Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Биометрия, смарткарты.

**Тема 9. Средства защиты информации в автоматизированных информационных системах**

Классификация систем. Основные средства защиты информации: технические, программные, криптографические, организационные, законодательные. Средства контроля физического доступа. Автоматизированные средства защиты информации. Системы управления политикой безопасности. Автоматизированные системы как объекты защиты информации. Современное состояние классификации автоматизированных систем. Вычислительные сети. Сетевые модели доступа данных. Архитектура «файл-сервер». Архитектура «клиент-сервер». Эталонная модель OSI. Масштабирование компьютерных сетей. Топология вычислительных сетей. Сегментация сложных локальных сетей. Персональные, локальные, корпративные, региональные и глобальные сети. Виртуальные сети. Автоматизированные системы управления. Классификация автоматизированных систем. Организация проектирования автоматизированных систем. Условия и режимы эксплуатации автоматизированных систем.

**Тема 10. Основы защиты данных персонального компьютера**

Организация рабочего места. Анализ возможных путей утечки информации. Программы контроля и разграничения доступа к информации. Задачи и общие принципы построения программ контроля и разграничения доступа к информации. Методы борьбы. Резервное копирование, контроль пользователей, защита файлов и папок.

Схема защиты ПК. Защита BIOS. Системы защиты паролями Windows. Профили и пароли пользователей. Выбор значений паролей. Выбор носителей кодов паролей. Разграничение полномочий пользователей. Концепция построения систем контроля и разграничения доступа. Средства перекрытия путей обхода программ контроля и разграничения доступа. Оценка программ контроля и разграничения доступа как

средства защиты. Контроль целостности программного обеспечения и информации. Дублирование информации. Средства защиты программного обеспечения и информации от несанкционированной загрузки. Защита информации на машинных носителях. Защита остатков информации. Защита информации в линиях связи. Защита информации при документировании. Удаленный доступ. Сетевая защита файлов и папок. Программы администрирования. Организационные мероприятия по защите информации в автоматизированных информационных системах.

**Тема 11. Основы безопасности в Интернете**

Угрозы. Классификация удаленных атак: по сценарию, по цели, по характеру взаимодействия с жертвой. Удаленный сбор информации. Выяснение адресов. Поиск уязвимостей. Наиболее распространенные классы удаленных атак. Вирусы и троянские программы. Отказ в обслуживании. Маскировка. Атаки на маршрутизацию. Атаки на серверы: CGI и HTTP. Атаки на клиентов: ActiveX, Java. Переполнение буфера.

Пассивные атаки. Прослушивание сетей. Прослушивание в коммутируемых сетях Ethernet. Активные атаки. Атака повтором. Атака «злоумышленник-посредник». Атаки на основе сетевой маршрутизации. Перехват сессии. Инструменты злоумышленников. Классификация программ-шпионов и защита от них. Особенности защиты информации в базах данных.

Обзор программных средств защиты. Обеспечение анонимности: службы анонимности, прокси-серверы. Сканеры уязвимости. Системы и технологии обнаружения атак. Топология систем обнаружения атак. Автоматизированные средства управления политикой безопасности.

Средства обеспечения безопасности работы в Интернете. Средства контроля и разграничения доступа. Программные шлюзы и прокси-серверы. Межсетевые экраны. Функции межсетевого экранирования. Фильтрация трафика. Средства защиты трафика.

**Тема 12. Методология построения защищенных автоматизированных информационных систем**

Критерии защищенности. Анализ и оценка действующей концепции защиты. Выбор концептуальной модели построения защиты. Исходные данные для постановки задачи. Введение в проблему теории защиты информации. Общий методический подход. Основные принципы построения защитной оболочки. Модель элементарной защиты. Модель многозвенной защиты. Многоуровневая защита. Некоторые особенности точности расчета прочности защиты. Метод построения защиты информации в системах с сосредоточенной обработкой данных. Классификация возможных каналов НСД. Метод построения защиты информации в системах с распределенной обработкой данных.

## 7. Фонд оценочных средств (ФОС) для оценивания результатов обучения по дисциплине (модулю).

### 7.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости.

**Контрольные вопросы и задания для самостоятельной работы по темам курса.**

**Тема 1. Введение в информационную безопасность**

Контрольные вопросы:

1. Данные и информация.
2. Свойства информации.
3. Виды и формы представления информации.

4. Информация как объект защиты.
5. Цели, механизмы, инструментарий, основные направления информационной безопасности.
Задание для самостоятельной работы:
Проведите дискуссию на предмет информации как объекта защиты.

**Тема 2. Обеспечение информационной безопасности общества как основа государственной информационной политики**

Контрольные вопросы:
1. Государственная информационная политика.
2. Особенности государственной информационной политики в современной России.
3. Информационная агрессия и способы её нейтрализации.
4. Виды обеспечения защиты информации.
Задание для самостоятельной работы:
Проведите дискуссию на предмет особенностей государственной информационной политики в современной России.

**Тема 3. Информационная безопасность как предмет философско-политологического осмысления**

Контрольные вопросы:
1. Определения понятия «безопасность» представителей разных философских школ.
2. Динамика развития понятийного аппарата «безопасность».
3. Классификация информационных систем и объектов, модель классификации.
Задание для самостоятельной работы:
Проведите дискуссию на предмет развития понятийного аппарата «безопасность».

**Тема 4. Информационная война: сущность, разновидности, средства и методы ведения**

Контрольные вопросы:
1. Понятия «информационная война», «информационное оружие».
2. Разновидности информационной войны.
3. Технологии манипулятивного воздействия.
4. Источники угроз.
5. Виды угроз.
Задание для самостоятельной работы:
Проведите дискуссию на предмет источников и видов информационных угроз.

**Тема 5. Информационная безопасность политического пространства**

Контрольные вопросы:
1. Понятие политическое пространство.
2. Информационное пространство политики.
3. Субъекты информационного пространства политики.
4. Принципы и технологии обеспечения информационной безопасности.

Задание для самостоятельной работы:
Проведите дискуссию о технологиях обеспечения информационной безопасности.

**Тема 6. Информационная ответственность субъектов политических отношений**

Контрольные вопросы:
1. Субъекты политики с точки зрения традиционной политологии.
2. Особенности и значение СМИ как субъекта политики на современном этапе развития общества.
3. Трансформация роли традиционных политических институтов.
4. Информационное пространство, порождаемое субъектом политики.

Задание для самостоятельной работы:
Проведите дискуссию о информационном пространстве субъекта политики.

**Тема 7. Экономика информационной безопасности**

Контрольные вопросы:
1. Объективные и субъективные вероятности реализации угроз посредством уязвимостей и их оценка.
2. Измерение рисков, шкалы рисков.
3. Технологии оценки угроз, уязвимостей, рисков и потерь.
4. Методика выбора компонентов системы защиты информации и предполагаемая оценка ее эффективности.
5. Экономические проблемы информационных ресурсов.
6. Экономическая безопасность.

Задание для самостоятельной работы:
Проведите дискуссию о технологиях оценки угроз, уязвимостей, рисков и потерь.

**Тема 8. Технические средства защиты информации**

Контрольные вопросы:
1. Устройства и системы противоправного преднамеренного овладения конфиденциальной информацией.
2. Технические средства защиты объектов.
3. Инженерно-техническая защита.
4. Методы и средства защиты информации от случайных воздействий.
5. Методы защиты информации от аварийных ситуаций.

Задание для самостоятельной работы:
Проведите дискуссию о технических средствах защиты информационных объектов.

**Тема 9. Средства защиты информации в автоматизированных информационных системах**

Контрольные вопросы:
1. Средства защиты информации: технические, программные, криптографические, организационные, законодательные.
2. Автоматизированные средства защиты информации.
3. Системы управления политикой безопасности.

4. Вычислительные сети.
5. Сетевые модели доступа данных.
6. Архитектура «файл-сервер».
7. Архитектура «клиент-сервер».
8. Эталонная модель OSI.
9. Персональные, локальные, корпративные, региональные и глобальные сети.
10. Виртуальные сети.

Задание для самостоятельной работы:

Проведите дискуссию о системах управления политикой безопасности.

**Тема 10. Основы защиты данных персонального компьютера**

Контрольные вопросы:

1. Возможные пути утечки информации.
2. Программы контроля и разграничения доступа к информации.
3. Резервное копирование, контроль пользователей, защита файлов и папок.
4. Системы защиты паролями Windows. Профили и пароли пользователей.
5. Разграничение полномочий пользователей.
6. Контроль целостности программного обеспечения и информации.
7. Дублирование информации.
8. Сетевая защита файлов и папок.
9. Программы администрирования.

Задание для самостоятельной работы:

Проведите дискуссию о целостности программного обеспечения и информации.

**Тема 11. Основы безопасности в Интернете**

Контрольные вопросы:

1. Классификация удаленных атак: по сценарию, по цели, по характеру взаимодействия с жертвой.
2. Классы удалённых атак.
3. Вирусы и троянские программы.
4. Отказ в обслуживании.
5. Атаки на маршрутизацию.
6. Атаки на серверы: CGI и HTTP.
7. Атаки на клиентов: ActiveX, Java.
8. Переполнение буфера.
9. Пассивные атаки.
10. Активные атаки.

11. Программные средства защиты.
12. Средства защиты трафика.
Задание для самостоятельной работы:
Проведите дискуссию о удалённых информационных атаках.

**Тема 12. Методология построения защищённых автоматизированных информационных систем**

Контрольные вопросы:
1. Критерии защищённости.
2. Выбор концептуальной модели построения защиты.
3. Основные принципы построения защитной оболочки.
4. Модель элементарной защиты.
5. Модель многозвенной защиты.
6. Многоуровневая защита.
7. Метод построения защиты информации в системах с распределённой обработкой данных.

Задание для самостоятельной работы:
Проведите дискуссию о критериях защищенности автоматизированных информационных систем.

**Тематика дискуссий.**

Дискуссии в курсе «Информационная безопасность» могут организовываться в трех случаях. Во-первых, выступать завершением отдельных разделов учебного курса, во-вторых, являться следствием возникших на занятиях дискуссионных проблем, которые могут быть вынесены в качестве тем дискуссий для специального углубленного осмысления и анализа. И, в-третьих, если учебная группа обучающихся составляет не менее 8-10 человек.

Целесообразными темами дискуссий могут быть:
1. Информация как объекта защиты.
2. Особенности государственной информационной политики в современной России.
3. Развитие понятийного аппарата «безопасность».
4. Источники и виды информационных угроз.
5. Технологии обеспечения информационной безопасности.
6. Информационное пространство субъекта политики.
7. Технологии оценки угроз, уязвимостей, рисков и потерь.
8. Технические средства защиты информационных объектов.
9. Системы управления политикой безопасности.
10. Целостность программного обеспечения и информации.
11. Удалённые информационные атаки.
12. Критерии защищённости автоматизированных информационных систем.

**Тематика эссе.**

1. Информация как объект защиты.
2. Особенности государственной информационной политики в современной России.
3. Развитие понятийного аппарата «безопасность».
4. Источники и виды информационных угроз.
5. Технологии обеспечения информационной безопасности.
6. Информационное пространстве субъекта политики.
7. Технологии оценки угроз, уязвимостей, рисков и потерь.
8. Технические средства защиты информационных объектов.
9. Системы управления политикой безопасности.
10. Целостность программного обеспечения и информации.
11. Удалённые информационные атаки.
12. Критерии защищенности автоматизированных информационных систем.

**7.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации.**

**Вопросы к зачёту.**

1. Данные и информация.
2. Свойства информации.
3. Виды и формы представления информации.
4. Информация как объект защиты.
5. Цели, механизмы, инструментарий, основные направления информационной безопасности.
6. Государственная информационная политика.
7. Особенности государственной информационной политики в современной России.
8. Информационная агрессия и способы её нейтрализации.
9. Виды обеспечения защиты информации.
10. Определения понятия «безопасность» представителей разных философских школ.
11. Динамика развития понятийного аппарата «безопасность».
12. Классификация информационных систем и объектов, модель классификации.
13. Понятия «информационная война», «информационное оружие».
14. Разновидности информационной войны.
15. Технологии манипулятивного воздействия.
16. Источники угроз.
17. Виды угроз.
18. Понятие политическое пространство.
19. Информационное пространство политики.

20. Субъекты информационного пространства политики.
21. Принципы и технологии обеспечения информационной безопасности.
22. Субъекты политики с точки зрения традиционной политологии.
23. Особенности и значение СМИ как субъекта политики на современном этапе развития общества.
24. Трансформация роли традиционных политических институтов.
25. Информационное пространство, порождаемое субъектом политики.
26. Объективные и субъективные вероятности реализации угроз посредством уязвимостей и их оценка.
27. Измерение рисков, шкалы рисков.
28. Технологии оценки угроз, уязвимостей, рисков и потерь.
29. Методика выбора компонентов системы защиты информации и предполагаемая оценка её эффективности.
30. Экономические проблемы информационных ресурсов.
31. Экономическая безопасность.
32. Устройства и системы противоправного преднамеренного овладения конфиденциальной информацией.
33. Технические средства защиты объектов.
34. Инженерно-техническая защита.
35. Методы и средства защиты информации от случайных воздействий.
36. Методы защиты информации от аварийных ситуаций.
37. Средства защиты информации: технические, программные, криптографические, организационные, законодательные.
38. Автоматизированные средства защиты информации.
39. Системы управления политикой безопасности.
40. Вычислительные сети.
41. Сетевые модели доступа данных.
42. Архитектура «файл-сервер».
43. Архитектура «клиент-сервер».
44. Эталонная модель OSI.
45. Персональные, локальные, корпоративные, региональные и глобальные сети.
46. Виртуальные сети.
47. Возможные пути утечки информации.
48. Программы контроля и разграничения доступа к информации.
49. Резервное копирование, контроль пользователей, защита файлов и папок.
50. Системы защиты паролями Windows. Профили и пароли пользователей.
51. Разграничение полномочий пользователей.
52. Контроль целостности программного обеспечения и информации.
53. Дублирование информации.

54. Сетевая защита файлов и папок.
55. Программы администрирования.
56. Классификация удаленных атак: по сценарию, по цели, по характеру взаимодействия с жертвой.
57. Классы удалённых атак.
58. Вирусы и троянские программы.
59. Отказ в обслуживании.
60. Атаки на маршрутизацию.
61. Атаки на серверы: CGI и HTTP.
62. Атаки на клиентов: ActiveX, Java.
63. Переполнение буфера.
64. Пассивные атаки.
65. Активные атаки.
66. Программные средства защиты.
67. Средства защиты трафика.
68. Критерии защищённости.
69. Выбор концептуальной модели построения защиты.
70. Основные принципы построения защитной оболочки.
71. Модель элементарной защиты.
72. Модель многозвенной защиты.
73. Многоуровневая защита.
74. Метод построения защиты информации в системах с распределенной обработкой данных.

**Критерии оценки ответов на зачёте:**

| | |
|---|---|
| Зачтено | Ответ логически выстроен и излагается на хорошем научном языке. Студент хорошо владеет необходимыми источниками и литературой, хорошо ориентируется в них, использует при ответе специализированную лексику, даёт хорошие ответы на основной и дополнительные вопросы. |
| Не зачтено | В ответе полностью отсутствует явная логика. Студент не владеет в полной мере даже основными источниками, не ориентируется в них, при ответе не использует специализированную лексику, даёт неудовлетворительные ответы на дополнительные и основные вопросы. |

**Шкала и критерии оценивания результатов обучения по дисциплине (модулю).**

| Индикатор | ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю) | | | | | |
|---|---|---|---|---|---|---|
| | Оценка / Результаты обучения | 2 | 3 | 4 | 5 | **Виды оценочных средств** |
| **ОПК-2.1 Использует информационно-коммуникационные технологии и программные средства для поиска, обработки информации по поставленной проблематике на основе принятых профессиональных норм и с учетом требований информационной безопасности** | **Знать** основы информационной безопасности. | Отсутствие знаний | Фрагментарные знания | Общие, но не структурированные знания | Сформированные систематические знания | Опрос по лекционному материалу (тема 8-12), зачёт |
| | **Знать** информационно-коммуникационные технологии | Отсутствие знаний | Фрагментарные знания | Общие, но не структурированные знания | Сформированные систематические знания | Опрос по лекционному материалу (тема 1-12), зачёт |
| | **Уметь** обоснованно отбирать ИКТ для поиска, обработки информации по поставленной проблематике | Отсутствие умений | В целом успешное, но не систематическое умение | В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера | Успешное и систематическое умение | дискуссия (см. тематика 1-12) эссе (см. тематика эссе 1-12) |
| | **Владеть** основами информационно-библиографической культуры | Отсутствие владения | В целом успешное, но не систематическое владения | В целом успешное, но содержащее отдельные пробелы владение (допускает неточности непринципиального характера) | Успешное и систематическое владение | Использование информационно-библиографических ресурсов при подготовке к занятиям (тема 1-12), зачету (вопросы) и написанию эссе (тематика 1-12) |

**8. Ресурсное обеспечение:**

**8.1. Учебно-методическое и информационное обеспечение дисциплины.**

**Перечень основной и дополнительной учебной литературы:**

**а) основная литература:**


1. Балдин, К.В. Информатика для ВУЗов: Учебник / К.В. Балдин, В.Б. Уткин. - М.: Дашков и К, 2016. - 395 с.
2. Бирюков А.Н. Процессы управления информационными технологиями [Электронный ресурс]: учебное пособие/ Бирюков А.Н.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.— 262 с.— Режим доступа: http://www.iprbookshop.ru/89467.html.— ЭБС «IPRbooks»
3. Ефимова,Лариса Львовна (). Информационная безопасность детей : рос. и зарубеж. опыт : монография / Л. Л. Ефимова, С. А. Кочерга М. : ЮНИТИ, 2013
4. Информатика : учеб. для бакалавров / [Трофимов В. В. и др.] ; под ред. В. В. Трофимова ; С. - Петерб. гос.ун-тэкономики и финансов М. : Юрайт, 2013
5. Историческая информатика : Учеб.пособие / Е.Б.Белова,Л.И.Бородкин,И.М.Гарскова и др.;Под ред.Л.И.Бородкина,И.М.Гарсковой М. : Мосгорархив, 1996
6. Ковалева Н.Н. Комментарий к ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]/ Ковалева Н.Н., Холодная Е.В.— Электрон. текстовые данные.— Москва: Новая правовая культура, 2008.— 257 с.— Режим доступа: http://www.iprbookshop.ru/1595.html.— ЭБС «IPRbooks»
7. Макарова Н. В. Информатика: Учебник для вузов. Издательство: Питер, 2013, 576 с.
8. Осипова,Надежда Геннадьевна (). Динамика представлений российской студенческой молодежи о социально-политических процессах, институтах социализации и субъектах осуществления молодежной политики в период с 2013 по 2017 г. / Н. Г. Осипова, С. О. Елишев, Г. Б. Прончев ; Моск. гос. ун-т им. М. В. Ломоносова, Социол. фак., Каф. соврем. социологии М. : Канон-плюс, 2018
9. Основы информационных технологий [Электронный ресурс]: учебное пособие/ С.В. Назаров [и др.].— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.— 530 с.— Режим доступа: http://www.iprbookshop.ru/89454.html.— ЭБС «IPRbooks».
10. Скворцов Л. В. Информационная культура и цельное знание / Л. В. Скворцов. М. : МБА, 2011.
11. Прончев Г.Б., Монахов Д.Н., Монахова Г.А. Информационные технологии в науке и образовании. – М. : МАКС Пресс, 2013.


**б) дополнительная литература:**


1. Бабаш,Александр Владимирович (). Актуальные вопросы защиты информации : монография / А. В. Бабаш, Е. К. Баранова М. : РИОР : ИНФРА-М, 2017 доп4
2. Баданов,Алексей Геннадьевич (). Информационная безопасность: от теории к практике : учеб. пособие / А. Г. Баданов ; Моск. гос. ун-т им. М. В. Ломоносова, Экон. фак. М. : Теис, 2010

3. Гасумова С.Е.— Электрон. текстовые данные.— М.: Дашков и К, 2019.— 311 с.— Режим доступа: http://www.iprbookshop.ru/85325.html.— ЭБС «IPRbooks»
4. Ершова Т. Информационное общество – это мы. – М. : Ин-т развития информ. о-ва, 2008
5. Журавлева Т.Ю. Информационные технологии [Электронный ресурс]: учебное пособие/ Журавлева Т.Ю.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 72 с.— Режим доступа: http://www.iprbookshop.ru/74552.html.— ЭБС «IPRbooks»
6. Иванов Д.В. Виртуализация общества: Версия 2.0 - СПб.: Петербургское Востоковедение, 2002. 96 с.
7. Капралов Е. Г., Кошкарев А. В., Тикунов В. С. и др. Геоинформатика. В 2-х кн. Учебн. для вузов.// Под ред. В.С.Тикунова. 2-е изд., перер. и доп. – М.: Академия, 2008. http://www.geokniga.org/bookfiles/geokniga-geoinformatikakapralov-koshkarev-tikunov-i-druchebnik2005-480s.pdf
8. Кастельс М. Галактика Интернет: Размышления об Интернете, бизнесе и обществе / Пер. с англ. А. Матвеева под ред. В. Харитонова. – Екатеринбург: У-Фактория, 2004.
9. Кастельс М. Информационная эпоха: Экономика, обществово и культура / Пер.с англ.под науч.ред.О.И.Шкаратана; Гос.ун-т Высш.шк.экономик. - М.: CEU, 2000.
10. Колин К.К. Философские проблемы информатики – М. : БИНОМ. Лаб. знаний, 2010.
11. Левин В.И. История информационных технологий [Электронный ресурс]: учебник/ Левин В.И.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.— 750 с.— Режим доступа: http://www.iprbookshop.ru/89440.html.— ЭБС «IPRbooks»
12. Ловцов, Д.А. Геоинформационные системы / Д.А. Ловцов, А.М. Черных. – М.: Российская академия правосудия, 2012. http://znanium.com/bookread2.php?book=517128&spec=1
13. Монахов Д.Н., Монахова Г.А., Прончев Г.Б., Прончева Н.Г. Практикум по информатике для студентов - социологов. Часть 1. – М. : Экон-Информ, 2014.
14. Патаракин Е.Д. Сетевые сообщества и обучение. – М.: PerSe, 2006.
15. Персова М.Г. Современные компьютерные технологии [Электронный ресурс]: конспект лекций/ Персова М.Г., Соловейчик Ю.Г., Домников П.А.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2014.— 80 с.— Режим доступа: http://www.iprbookshop.ru/45025.html.— ЭБС «IPRbooks»
16. Петров М.Н., Молочков В.П. Компьютерная графика. Компьютерная графика : Учеб.пособие для студентов вузов / М.Н.Петров,В.П.Молочков и др. – С.Пб.: Питер, 2004.
17. Плотинский Ю.М. Модели социальных процессов. – М.: Логос, 2001.
18. Прончев Г.Б., Монахов Д.Н., Монахов Н.В. Практикум по информатике для студентов - социологов. Часть 2. Поиск информации. . – М. : Экон-Информ, 2014 15. Рунов А.В. Социальная информатика. – М.: КноРус, 2009.
19. Современные компьютерные технологии [Электронный ресурс]: учебное пособие/ Р.Г. Хисматов [и др.].— Электрон. текстовые данные.— Казань: Казанский национальный исследовательский технологический университет, 2014.— 83 с.— Режим доступа: http://www.iprbookshop.ru/62279.html.— ЭБС «IPRbooks»
20. Уэбстер Ф. Теории информационного общества. – М.: Аспект Пресс, 2004.

21. Цветкова А.В. Информатика и информационные технологии [Электронный ресурс]: учебное пособие/ Цветкова А.В.— Электрон. текстовые данные.— Саратов: Научная книга, 2012.— 189 с.— Режим доступа: http://www.iprbookshop.ru/6276.html.— ЭБС «IPRbooks»
22. Штомпка П. Визуальная социология. Фотография как метод исследования: учебник/ пер. с польск. Н.В. Морозовой, авт. вступ. ст. Н.Е. Гасумова С.Е. Информационные технологии в социальной сфере [Электронный ресурс]: учебное пособие для бакалавров/
23. Ярочкин В.И. Информационная безопасность: учеб. для студентов вузов / В.И. Ярочкиню М.: Акад. проект, 2008.

**Перечень лицензионного программного обеспечения.**
Обязательное программное обеспечение – MS Office.

**Перечень профессиональных баз данных, информационных справочных систем. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»**

**Интернет-ресурсы:**

1. Сайт «Социальная информатика» http://soc-inform4.narod.ru/
2. Федеральный портал «Российское образование» http://www.edu.ru/
3. Федеральный образовательный портал» http://www.ecsocman.edu.ru/
4. Научная библиотека МГУ http://www.nbmgu.ru
5. Электронная библиотека iprbooks http://www.iprbookshop.ru

**Описание материально-технического обеспечения:**

- проведение лекционных занятий требуется аудитория с трансформируемым пространством, оборудованная компьютером и проектором, необходимыми для демонстрации презентаций. Обязательное программное обеспечение – MS Office;
- проведение аудиторных занятий с использованием информационно-коммуникационных мультимедийных технологий;
- обеспечение студентов сопутствующими раздаточными материалами – опорными конспектами с целью активизации работы студентов по усвоению материалов учебного курса;
- использование интерактивных обучающих технологий: научные семинары, дискуссии, круглые столы, презентации в Power Point.

**9.Язык преподавания.**
Русский.

**10. Преподаватель.**
Монахов Д.Н., доцент

**11. Разработчики программы.**

Прончев Г.Б., доцент, к.физ.-мат. н.
Гончарова И.В., доцент, пед. н.