МИНОБРНАУКИ РОССИИ

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

ИСТОРИКО-АРХИВНЫЙ ИНСТИТУТ
ИСТОРИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра всеобщей истории

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ИНФОРМАЦИОННЫЙ СУВЕРЕНИТЕТ: ПРАВОВЫЕ И СОЦИАЛЬНЫЕ АСПЕКТЫ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

46.04.01 История
Код и наименование направления подготовки/специальности

Искусственный интеллект и цифровые технологии в исторических исследованиях
Наименование направленности (профиля)/ специализации

Уровень высшего образования: магистратура

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2026

Информационная безопасность, информационный суверенитет: правовые и социальные аспекты
Рабочая программа дисциплины

Составители:
к.э.н., доц., заведующий кафедрой фундаментальной
и прикладной математики, А.Ю. Журавлев

УТВЕРЖДЕНО
Протокол заседания кафедры фундаментальной и прикладной математики
№ 8 от 06.12.2025

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: сформировать у студентов-гуманитариев целостное понимание современных вызовов и угроз в цифровой среде, правовых механизмов их регулирования, а также социально-философских оснований концепций информационной безопасности и суверенитета, необходимых для критического анализа цифрового пространства и выработки стратегий профессиональной деятельности в условиях цифровой трансформации исторической науки.

Задачи дисциплины:

- Раскрыть сущность и многогранность понятий «информационная безопасность» и «информационный суверенитет» в междисциплинарной перспективе (технической, правовой, социально-гуманитарной).
- Изучить основные виды угроз информационной безопасности (кибератаки, дезинформация, манипуляция сознанием, утечки данных) и их потенциальное влияние на общество, историческую память и научные исследования.
- Сформировать представление об основах российского и международного права в сфере информационной безопасности, защиты персональных данных, интеллектуальной собственности и регулирования цифрового пространства.
- Проанализировать социальные, этические и политические аспекты информационного суверенитета, цифрового неравенства, свободы информации и цензуры в глобальном и национальном контекстах.
- Развить навыки критической оценки информационных угроз, анализа правовых кейсов и разработки базовых рекомендаций по обеспечению информационной безопасности в профессиональной деятельности историка.

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

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Осуществляет критический анализ проблемных ситуаций на основе системного подхода, вырабатывает стратегию действий, формулирует научно обоснованные гипотезы, применяет методологию научного познания в профессиональной деятельности	**Знать:** основные концепции и методологии анализа цифрового общества (сетевой анализ, теория медиа, политическая экономия коммуникаций); ключевые социальные теории, объясняющие природу информационных угроз и манипуляций; философские основания дискуссий о свободе информации, приватности и суверенитете в цифровую эпоху. **Уметь:** выявлять и систематизировать различные типы угроз информационной безопасности в конкретных профессиональных и

		общественных контекстах; анализировать комплексные проблемные ситуации на стыке технологий, права и социума (например, кейсы с утечками исторических архивов или цифровым вандализмом); формулировать научно обоснованные гипотезы о причинах и возможных последствиях информационных инцидентов; разрабатывать стратегические рекомендации по минимизации рисков для исследовательских проектов и публичных исторических инициатив. **Владеть:** методологией системного анализа сложных социотехнических систем; навыками критической оценки источников информации и верификации цифрового контента; техниками сценарного прогнозирования (форсайта) для оценки долгосрочных социальных последствий технологических решений в информационной сфере.
ПК-7. Способен осуществлять критический анализ проблемных ситуаций в сфере интерпретации и репрезентации истории России в современном информационном пространстве, базовых дискурсов и нарративов, оценивать их влияние на историко-культурные и общественно-политические процессы	ПК-7.2. Демонстрирует знание принципов функционирования современного информационного пространства, его взаимосвязи и взаимовлияния с человеком и обществом	**Знать:** базовые технические принципы функционирования ключевых элементов информационного пространства (интернет-архитектура, большие данные, алгоритмы рекомендательных систем, технологии блокчейн в контексте аутентификации); основные положения российского законодательства в области информационной безопасности (ФЗ-152 «О персональных данных», ФЗ-149 «Об информации, информационных технологиях и о защите информации», ФЗ-187 «О безопасности критической информационной инфраструктуры», «Стратегия национальной безопасности»); основы

		международного права и этические кодексы, регулирующие цифровую среду. **Уметь:** анализировать, как технологические особенности цифровых платформ (алгоритмы, монетизация внимания) формируют информационные потоки и влияют на общественное мнение и историческое сознание; применять знание правовых норм для оценки законности действий различных акторов в информационном пространстве (государств, корпораций, исследователей); оценивать риски, связанные с обработкой персональных и исторических данных в исследовательской работе. **Владеть:** навыками поиска и анализа актуальных нормативно-правовых актов в сфере ИБ; базовой терминологией в области кибербезопасности и цифрового права для профессиональной коммуникации; методикой составления карты стейкхолдеров и их интересов в конкретных ситуациях, связанных с информационным суверенитетом.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность, информационный суверенитет: правовые и социальные аспекты» относится к элективным дисциплинам части, формируемой участниками образовательных отношений. Необходимы знания, умения и владения, сформированные в результате изучения дисциплин «Цифровые технологии в архивном деле. Электронные архивы», «Информационные системы и базы данных: структурирование исторической информации». В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения последующих дисциплин как обязательной части учебного плана, так и части, формируемой участниками образовательных отношений.

2. Структура дисциплины

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

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
1	Лекции	14
1	Семинары	14
	Всего:	28

Объем дисциплины в форме самостоятельной работы обучающихся составляет 66 академических часов.

Структура дисциплины для очно-заочной 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
1	Лекции	12
1	Семинары	12
	Всего:	24

Объем дисциплины в форме самостоятельной работы обучающихся составляет 84 академических часа.

Структура дисциплины для заочной 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
1	Лекции	6
1	Семинары	2
2	Семинары	4
	Всего:	12

Объем дисциплины в форме самостоятельной работы обучающихся составляет 52 академических часа.

3. Содержание дисциплины

Раздел 1. Концептуальные основы: информация, безопасность, суверенитет в цифровую эпоху.

Тема 1.1. Введение. Информационное общество: от утопии к дистопии. Аннотация: Эволюция понятий «информационное общество» и «общество знаний». Ключевые характеристики цифровой эпохи: глобальная связанность, данные как новый ресурс, скорость коммуникации. Социологический и философский взгляд на трансформацию социальных институтов (власть, знание, память) под влиянием цифровых технологий. Постановка ключевых проблем курса: приватность vs. безопасность, свобода vs. контроль, глобальное vs. национальное

в киберпространстве. Информационная безопасность как комплексная проблема на стыке технологий, права, психологии и социологии.

Тема 1.2. Информационная безопасность: многоуровневая модель. Аннотация: Классическая триада КЦД (конфиденциальность, целостность, доступность) и ее расширение в современных условиях (аутентичность, неотказуемость, подотчетность). Уровни обеспечения ИБ: личностный, корпоративный, государственный, международный. Переход от защиты информации к обеспечению безопасности информационной среды и психологического состояния общества. Информационно-психологическая безопасность как ключевой вызов для гуманитария. Основные категории угроз: киберугрозы (вредоносное ПО, атаки), информационно-психологические (дезинформация, пропаганда, манипуляция), социотехнические (фишинг, социальная инженерия).

Тема 1.3. Информационный суверенитет: история, трактовки, дискурс. Аннотация: Генезис понятия «суверенитет» и его адаптация к цифровой сфере. Основные подходы к информационному суверенитету: как к техническому контролю над инфраструктурой, как к праву регулировать контент на своей территории, как к способности защищать цифровую идентичность граждан. Сравнительный анализ концепций «цифрового суверенитета» в России, ЕС, Китае, США. Критика концепции: обвинения в цифровом протекционизме и нарушении прав человека. Информационный суверенитет vs. глобальная открытость интернета: поиск баланса.

Раздел 2. Угрозы и вызовы: от данных к сознанию.

Тема 2.1. Технические основы и киберугрозы для гуманитария. Аннотация: Упрощенное объяснение ключевых технологий: IP-адресация, шифрование, блокчейн, VPN. Основные векторы кибератак: фишинг, ransomware (вымогатели), DDoS-атаки. Чем опасны утечки баз данных для исторических исследований и архивов? Понятие «критическая информационная инфраструктура» (КИИ) и ее значение для сохранения культурного наследия. Основы «цифровой гигиены» для исследователя: управление паролями, двухфакторная аутентификация, осторожность с публичным Wi-Fi.

Тема 2.2. Большие данные, слежка и приватность: «Дивный новый цифровой мир». Аннотация: Феномен big data и его применение в социальных науках и бизнесе. Технологии слежки: куки, цифровые отпечатки, распознавание лиц, метаданные. Бизнес-модели, основанные на сборе и анализе данных. Концепции «капитализма слежки» (Шошанна Зубофф) и «общества контроля» (Делёз). Кейсы утечек и злоупотреблений данными (Cambridge Analytica). Право на забвение и его реализация. Приватность как социальная ценность и правовая категория в исторической перспективе.

Тема 2.3. Информационные операции, дезинформация и историческая память. Аннотация: Информационная война и информационные операции: цели, методы, каналы. Технологии создания и распространения фейковых новостей, глубоких подделок (deepfakes). Использование исторических нарративов и символов в пропаганде. Феномен «войн памяти» в цифровом пространстве. Историк как целевая аудитория и потенциальная жертва манипуляций. Роль социальных сетей и алгоритмов в поляризации общества и распространении дезинформации. Методы верификации информации и факт-чекинга.

Раздел 3. Правовое регулирование и управление информационным пространством.

Тема 3.1. Российское законодательство в сфере информационной безопасности: основы. Аннотация: Система ключевых законов: ФЗ-149 (об информации), ФЗ-152 (о персональных данных), ФЗ-187 (о КИИ), ФЗ-436 (о защите детей). Основные понятия: информационная

система, оператор персональных данных, запрещенная информация, правообладатель. Требования к обработке персональных данных: согласие, обезличивание, трансграничная передача. Правовые основания блокировки сайтов и контента. Обязанности организаций, в том числе научных и образовательных.

Тема 3.2. Международное право и этика в киберпространстве.
Аннотация: Проблема применения международного права (Устав ООН, Женевские конвенции) к киберпространству. Инициативы ООН, ОБСЕ, Совета Европы по регулированию поведения государств в цифровой среде. Будапештская конвенция о киберпреступности и альтернативные подходы. Корпоративная этика и саморегулирование (правила соцсетей, стандарты для ИИ). Этические кодексы для исследователей, работающих с цифровыми данными и историческим контентом.

Тема 3.3. Интеллектуальная собственность, открытый доступ и научные коммуникации.
Аннотация: Авторское право в цифровую эпоху. Понятия открытого доступа (Open Access), открытых данных (Open Data) и открытых образовательных ресурсов (OER). Лицензии Creative Commons. Пиратство и легальные альтернативы. Как правовые режимы ИС влияют на доступ к историческим источникам и распространение научных знаний? Движение за открытую науку (Open Science) и его значение для исторических исследований. Планы научных издательств (Elsevier, Springer) и проблема «огораживания» знаний.

Раздел 4. Социальные практики и будущее информационной безопасности.

Тема 4.1. Социология и психология цифровой безопасности: культура, доверие, резильентность.
Аннотация: Формирование культуры информационной безопасности в организации и обществе. Психологические факторы уязвимости: когнитивные искажения, доверчивость, эффект «спирали молчания». Социальное доверие к институтам в условиях информационной атаки. Концепция социальной резильентности (устойчивости) к дезинформации. Роль медиаграмотности и цифровой грамотности как «вакцины» против информационных угроз. Просветительские и образовательные практики.

Тема 4.2. Цифровое неравенство, доступ к информации и информационная справедливость.
Аннотация: Цифровой разрыв (digital divide) внутри стран и между странами: доступ, навыки, результаты. Информационная бедность и ее социальные последствия. Проблема «информационной перегрузки» (infobesity) и цифрового детокса. Доступ к информации как право человека и общественное благо. Концепция информационной справедливости (information justice). Как цифровое неравенство влияет на исторические исследования и формирование коллективной памяти?

Тема 4.3. Искусственный интеллект и будущее ИБ: новые вызовы и возможности.
Аннотация: Применение ИИ в кибербезопасности (поиск уязвимостей, обнаружение аномалий) и для создания угроз (генерация фейков, целевой фишинг). Этические проблемы алгоритмического принятия решений, профилирования и предвзятости ИИ. Проблема «черного ящика» и подотчетности ИИ-систем. Нормативное регулирование ИИ (Европейский акт об ИИ, российские инициативы). Сценарии будущего: усиление контроля или новые инструменты для защиты свободы и приватности?

Тема 4.4. Заключение. Стратегии и практики историка в небезопасном цифровом мире.
Аннотация: Интеграция полученных знаний. Разработка личной и профессиональной стратегии информационной безопасности для историка: работа с источниками, данными, коммуникация в научной среде, публичная деятельность. Роль историка как эксперта по верификации

информации и критика манипуляций с прошлым. Позиция исследователя в публичных дискуссиях об информационном суверенитете и цифровых правах. Обзор актуальных трендов и направлений для дальнейшего изучения.

4. Образовательные технологии

Для проведения учебных занятий по дисциплине используются различные образовательные технологии. Для организации учебного процесса может быть использовано электронное обучение и (или) дистанционные образовательные технологии.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Текущий контроль

При оценивании докладов и участия в дискуссии на семинаре (максимальная оценка – 4 баллов) учитываются:

- степень раскрытия содержания материала (2 балла);
- изложение материала (грамотность речи, точность использования терминологии и символики, логическая последовательность изложения материала (1 балл);
- знание теории изученных вопросов, сформированность и устойчивость используемых при ответе умений и навыков (1 балла).

При оценивании результатов критического анализа текста исторических источников (максимальная оценка – 4 балла) учитывается:

- основательность проведённой критики источника (1 балл);
- уровень понимания извлечённой из текста источника информации (2 балла);
- грамотность и логичность изложения аналитических суждений (1 балл).

При оценивании исторического эссе (максимальная оценка – 20 баллов) учитывается:

- уровень использования научно-исследовательской литературы по теме (6 баллов);
- самостоятельность и аргументированность рассуждения по центральной проблеме эссе (10 баллов);
- грамотность и логичность письменного текста (4 балла).

Промежуточная аттестация (зачет)

При проведении промежуточной аттестации студент должен ответить на 2 вопроса теоретического характера.

При оценивании ответа на каждый из теоретических вопросов учитывается:

- полнота и правильность ответа (4-5 баллов за каждый из вопросов);
- аргументированность выводов (3-4 балла за каждый из вопросов);
- уровень понимания учебного материала (5-6 баллов за каждый из вопросов);
- грамотность и логичность изложения материала (4-5 баллов за каждый из вопросов).

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:

<table>
<tr><td>100-балльная шкала</td><td colspan="2">Традиционная шкала</td><td>Шкала ECTS</td></tr>
<tr><td>95 – 100</td><td rowspan="2">отлично</td><td rowspan="4">зачтено</td><td>A</td></tr>
<tr><td>83 – 94</td><td>B</td></tr>
<tr><td>68 – 82</td><td>хорошо</td><td>C</td></tr>
<tr><td>56 – 67</td><td>удовлетворительно</td><td>D</td></tr>
</table>

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	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	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. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно	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	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

Контрольные вопросы для промежуточной аттестации в форме зачета:

1. Информационное общество: сущность, характеристики и ключевые проблемы безопасности.
2. Многоуровневая модель информационной безопасности: от защиты данных к безопасности личности и общества.
3. Концепция информационного суверенитета: основные трактовки, политический дискурс и критика.
4. Основные виды киберугроз и их специфика для сферы гуманитарных наук и исторических исследований.
5. «Капитализм слежки» и экономика больших данных: угрозы приватности и автономии личности.
6. Информационные операции и манипуляция историческим сознанием в цифровую эпоху.
7. Российское законодательство в сфере информационной безопасности: система ключевых законов и их значение.
8. Международно-правовое регулирование киберпространства: вызовы и современные инициативы.
9. Интеллектуальная собственность, авторское право и движение за открытую науку (Open Science).
10. Психологические и социальные факторы уязвимости к информационным угрозам. Культура информационной безопасности.
11. Цифровое неравенство как проблема информационной безопасности и социальной справедливости.
12. Этические и правовые вызовы, связанные с развитием искусственного интеллекта.
13. Историк в цифровую эпоху: профессиональные риски и стратегии обеспечения информационной безопасности.

Оценочные средства (материалы) для текущего контроля успеваемости
Вопросы закрытого типа (с одним верным вариантом ответа):

1. **Классическая триада информационной безопасности (КЦД) включает:**
   а) Качество, Ценность, Доступность
   б) Конфиденциальность, Целостность, Достоверность
   в) Конфиденциальность, Целостность, Доступность
   г) Контроль, Цифровизация, Доверие
2. **Фишинг — это вид киберугрозы, направленный на:**
   а) Вывод из строя сайта путем перегрузки трафиком
   б) Шифрование данных с целью выкупа
   в) Кражу конфиденциальной информации путем маскировки под доверенное лицо
   г) Уничтожение аппаратной части компьютера
3. **Основным нормативным актом, регулирующим обработку персональных данных в РФ, является:**
   а) ФЗ-149 «Об информации...»
   б) ФЗ-152 «О персональных данных»

в) ФЗ-187 «О безопасности КИИ»
г) Уголовный кодекс РФ

4. **Концепция «капитализма слежки» (Ш. Зубофф) описывает бизнес-модель, основанную на:**
   а) Производстве цифровых устройств
   б) Извлечении прибыли из предсказания и изменения человеческого поведения через сбор личных данных
   в) Разработке свободного программного обеспечения
   г) Платежах за подписку на онлайн-сервисы
5. **«Право на забвение» в цифровой среде предполагает:**
   а) Право на уничтожение любого неугодного контента
   б) Возможность требовать от поисковых систем удаления ссылок на устаревшую или нерелевантную личную информацию
   в) Запрет на хранение исторических архивов в цифровой форме
   г) Обязательное шифрование всех личных сообщений
6. **Информационный суверенитет государства чаще всего понимается как:**
   а) Полный запрет на использование иностранного программного обеспечения
   б) Способность государства контролировать информационные потоки на своей территории и защищать национальные интересы в цифровой сфере
   в) Обязанность граждан использовать только государственные информационные ресурсы
   г) Право на беспрепятственный доступ ко всей информации в интернете
7. **Deepfake (глубокая подделка) — это технология, использующая ИИ для:**
   а) Создания сверхсложных паролей
   б) Анализа больших данных
   в) Реалистичной подмены лица или голоса человека на видео или в аудиозаписи
   г) Защиты от DDoS-атак
8. **Критическая информационная инфраструктура (КИИ) — это:**
   а) Все серверы, находящиеся на территории страны
   б) Информационные системы и сети, нарушение функционирования которых может нанести ущерб безопасности государства
   в) Социальные сети с аудиторией более 1 млн пользователей
   г) Личные компьютеры государственных служащих
9. **Лицензия Creative Commons BY-SA позволяет:**
   а) Использовать произведение только в личных целях
   б) Свободно использовать и изменять произведение при условии указания авторства и распространения производных работ на тех же условиях
   в) Использовать произведение в коммерческих целях без каких-либо ограничений
   г) Полностью запрещает любое использование произведения
10. **Медиаграмотность в контексте информационной безопасности — это:**
    а) Умение программировать
    б) Способность критически анализировать медиасообщения, определять их достоверность, цели и возможные манипулятивные приемы
    в) Навык создания видеоконтента
    г) Знание всех законов о СМИ

Вопросы открытого типа (на размышление и понимание):

1. Объясните, почему проблема информационной безопасности вышла далеко за рамки чисто технической дисциплины и стала острой социально-гуманитарной проблемой. Приведите примеры.
2. В чем заключается основное противоречие между принципом свободы информации и концепцией информационного суверенитета? Как, на ваш взгляд, можно искать баланс между ними?
3. Проанализируйте кейс с утечкой персональных данных. Какие права граждан были нарушены? Какие правовые механизмы защиты они могут использовать в РФ?
4. Опишите, как технологии «больших данных» и алгоритмы рекомендательных систем социальных сетей могут влиять на формирование общественного мнения по историческим вопросам (например, о значении того или иного события).
5. Что такое «войны памяти» в цифровом пространстве? Приведите конкретный пример и проанализируйте инструменты, используемые сторонами.
6. Сформулируйте основные этические дилеммы, с которыми сталкивается историк при работе с оцифрованными архивами, содержащими личные данные людей XX века.
7. Каковы могут быть долгосрочные социальные последствия широкого распространения технологий глубоких подделок (deepfakes) для исторической науки и общественного доверия к аудиовизуальным свидетельствам?
8. Разработайте план простых мер «цифровой гигиены» для исследовательского проекта, предполагающего сбор интервью (персональные данные) и работу с чувствительными историческими документами.
9. Объясните, как цифровое неравенство (digital divide) может искажать исторические исследования, которые все больше опираются на оцифрованные источники и Big Data.
10. Какие навыки и знания, полученные в рамках этой дисциплины, будут наиболее востребованы в профессиональной деятельности историка через 10 лет? Аргументируйте свой ответ.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Основная литература:

1. **Введение в информационную безопасность: учебное пособие для гуманитариев** / Под ред. А.И. Смирнова. – М.: Проспект, 2023. – 288 с.
2. **Расторгуев, С.П. Информационная война и безопасность** / С.П. Расторгуев. – М.: Вильямс, 2021. – 320 с.
3. **Солдатов, А.А. Цифровой суверенитет: теория и практика** / А.А. Солдатов, И.В. Бороган. – М.: Альпина Паблишер, 2022. – 356 с.
4. **Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»** (в действ. ред.).
5. **Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»** (в действ. ред.).

Дополнительная литература:

1. **Зубофф, Ш. Эпоха надзорного капитализма: Битва за будущее человечества на новой границе власти** / Ш. Зубофф. – М.: Издательство Института Гайдара, 2022. – 800 с.

2. **Москалева, Е.Н. Право в цифровую эпоху** / Е.Н. Москалева. – М.: Норма, 2023. – 256 с.
3. **Поздняков, А.И. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты** / А.И. Поздняков. – М.: Когито-Центр, 2021. – 240 с.
4. **Соломон, П. Дипфейки: Искусственный интеллект и будущее правды** / П. Соломон. – СПб.: Питер, 2023. – 304 с.
5. **Шерстюк, В.П. Информационное общество и проблемы безопасности** / В.П. Шерстюк. – М.: Юрайт, 2022. – 198 с.

Интернет-ресурсы:

1. **Роскомнадзор:** https://rkn.gov.ru/ – Официальный сайт федерального органа исполнительной власти, осуществляющего контроль и надзор в сфере информационных технологий и связи.
2. **ФСТЭК России:** https://www.fstec.ru/ – Федеральная служба по техническому и экспортному контролю. Документы по защите информации.
3. **Коалиция за цифровую безопасность (CyberPeace Institute):** https://cyberpeaceinstitute.org/– Международная неправительственная организация, аналитика и отчеты.
4. **Creative Commons Россия:** https://ru.creativecommons.org/ – Информация об открытых лицензиях.
5. **«КиберЛенинка»:** https://cyberleninka.ru/ – Научная электронная библиотека открытого доступа с материалами по теме.

6.2 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://www.rsuh.ru/liber/resources.php

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для проведения аудиторных занятий необходим стандартный набор специализированной учебной мебели и учебного оборудования, в том числе аудиторная доска (с магнитной поверхностью и набором приспособлений для крепления демонстрационных материалов), экран (на штативе или навесной). Для проведения семинаров, а также организации самостоятельной работы студентов необходим компьютерный класс с рабочими местами, обеспечивающими выход в Интернет. Кроме того, для информационно-ресурсного обеспечения семинаров необходим доступ к сканеру, копировальному аппарату и принтеру.

Реализация учебной программы должна обеспечиваться доступом каждого студента к информационным ресурсам – университетскому библиотечному фонду и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе необходимо наличие программного обеспечения, позволяющего осуществлять поиск информации в сети Интернет, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Adobe Master Collection
4. Kaspersky Endpoint Security

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

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 семинарских занятий

Общие методические рекомендации для подготовки к семинарским занятиям: Семинары сочетают дискуссии, case-study (разбор конкретных кейсов), работу с нормативно-правовыми актами и проектную деятельность. Студенты заранее знакомятся с обязательными материалами (статьи, тексты законов, описания кейсов). Активность на семинаре оценивается через участие в обсуждении, умение аргументировать позицию, качество анализа кейса и презентации группового проекта. Особое внимание уделяется умению переводить технические и правовые понятия на язык социально-гуманитарного анализа.

Тема 1: Карта угроз: что угрожает историку в цифровом мире?
Вопросы для обсуждения:

1. Составьте классификацию угроз информационной безопасности, с которыми может столкнуться исследователь-историк (на всех уровнях: личном, профессиональном, институциональном).
2. Проанализируйте реальный кейс утечки/потери исторических данных (например, пожар в институте, хакерская атака на архив). Какие компоненты триады КЦД были нарушены? Каковы могли быть причины и последствия?
3. «Цифровая гигиена»: разработайте памятку из 5-7 ключевых правил для начинающего исследователя.

Тема 2: Большой Брат vs. Цифровая автономия: границы приватности.
Вопросы для обсуждения:

1. На основе концепции Ш. Зубофф проанализируйте, как бизнес-модели Google или Facebook превращают пользовательские данные в товар. Где проходит грань между персонализацией сервиса и манипуляцией?
2. Кейс «Cambridge Analytica»: как данные из соцсетей были использованы для политического влияния? Какие уроки из этого можно извлечь для анализа исторических электоральных процессов?
3. Обсудите этическую дилемму: имеет ли право историк будущего анализировать сегодняшние открытые данные соцсетей для реконструкции социальной жизни начала XXI века?

Тема 3: Войны памяти 2.0: фейки, deepfakes и исторические нарративы.
Вопросы для обсуждения:

1. Найдите в современном медиапространстве пример использования исторического события/образа в целях пропаганды или манипуляции. Проанализируйте использованные приемы.
2. Что такое «deepfake» и как эта технология ставит под сомнение достоверность аудиовизуальных исторических источников будущего?
3. Практикум по факт-чекингу. На основе предоставленных материалов (статья, пост в соцсети) разработайте алгоритм проверки достоверности заявленных исторических фактов.

Тема 4: Правовое поле: закон и цифровая реальность (работа с текстами законов).
Вопросы для обсуждения:

1. На основе ФЗ-152 определите, является ли исследователь, собирающий биографические интервью, оператором персональных данных. Какие обязанности у него возникают?
2. Проанализируйте ст. 15.3 ФЗ-149 («Единый реестр запрещенной информации»). Какие виды информации могут быть включены? Каковы возможные социальные последствия такого регулирования для исторических дискуссий?
3. Сравните подходы к регулированию «права на забвение» в РФ и в ЕС (Регламент GDPR). В чем сходства и различия?

Тема 5: Кому принадлежит прошлое? Интеллектуальная собственность и открытый доступ.
Вопросы для обсуждения:

1. Кейс: Музей выкладывает в открытый доступ оцифрованные рукописи XVIII века. Кто обладает авторскими правами: музей, оцифровавший документ, или наследники автора? Проанализируйте ситуацию.
2. Обсудите плюсы и минусы модели открытого доступа (Open Access) для научных исторических журналов. Как это влияет на развитие науки?
3. Практическая работа: выберите лицензию Creative Commons для своего гипотетического научно-популярного исторического блога. Обоснуйте выбор.

Тема 6: Социология кибербезопасности: почему люди становятся жертвами?
Вопросы для обсуждения:

1. Обсудите психологические механизмы, лежащие в основе успеха фишинговых атак и теорий заговора (например, когнитивные искажения, потребность в простых объяснениях).
2. Что такое «культура информационной безопасности» и как ее можно формировать в академической среде (на факультете, в исследовательском центре)?
3. Ролевая игра: разработайте сценарий просветительской беседы со школьниками о критическом восприятии исторической информации в интернете.

Тема 7: Цифровой разлом: неравенство и доступ к знанию.
Вопросы для обсуждения:

1. Как «цифровой разрыв» между странами и внутри стран влияет на глобальную историографию? Может ли это привести к новой форме «научного колониализма»?
2. Стоит ли государство обеспечивать бесплатный доступ к национальным оцифрованным архивным фондам? Аргументы «за» и «против».
3. Проект: предложите меры по преодолению цифрового неравенства в доступе к историческим источникам для региональных исследователей.

Тема 8: Искусственный интеллект: друг или враг историка?
Вопросы для обсуждения:

1. Обсудите возможности и риски использования ИИ в исторических исследованиях (например, для анализа текстов, атрибуции, создания цифровых реконструкций).
2. Кейс: алгоритм рекомендаций YouTube усиленно рекомендует пользователю, интересующемуся историей Второй мировой войны, контент радикального содержания. В чем проблема и кто несет ответственность?
3. Сформулируйте этические принципы, которые должны соблюдаться при разработке и применении ИИ-инструментов в гуманитарных науках.

Тема 9: Стратегирование: как историку выжить и сохранить суверенитет в цифровом мире? (Подготовка итоговых проектов).

Задание:

Работа в мини-группах над проектом «Кодекс информационной безопасности и этики для современного историка». Проект должен включать:

1. Анализ ключевых профессиональных рисков.
2. Раздел с практическими рекомендациями (работа с данными, коммуникация, публикации).
3. Этический раздел (взаимодействие с информационным пространством, ответственность за распространяемый контент).
4. Правовой минимум (на что обращать внимание в законах).

Тема 10: Презентация и защита проектов «Кодекс информационной безопасности...».

Формат:

Краткая презентация проекта каждой группой (10 мин.), ответы на вопросы и общая дискуссия. Обсуждение универсальных принципов и ситуативной специфики. Подведение итогов курса.

9.2 Методические рекомендации по подготовке письменных работ

Итоговой письменной работой по дисциплине является **аналитическое эссе**, посвященное комплексному разбору конкретной проблемы на стыке информационной безопасности, права и социальных практик, актуальной для исторической науки и смежных гуманитарных областей.

Цель эссе – продемонстрировать умение применять системный подход, знания правовых норм и социально-гуманитарных теорий для критического анализа сложной ситуации (кейса) и формулирования обоснованных выводов.

Структура эссе:

- **Введение (1-1.5 стр.):** Четкая формулировка выбранной проблемы/кейса. Обоснование ее актуальности для историка и общества в целом. Постановка цели и конкретных задач анализа.
- **Основная часть (3-4 стр.):** Последовательное решение поставленных задач.
    - **Аналитический раздел:** Системное описание кейса. Выявление и классификация задействованных сторон (стейкхолдеров), их интересов и действий. Анализ применяемых технологий, правовых норм (российских и/или международных) и социальных механизмов. Использование релевантных теорий (например, концепций информационного суверенитета, капитализма слежки, теорий медиа).
    - **Оценочный раздел:** Критическая оценка ситуации. Выявление ключевых противоречий (например, между свободой информации и правом на приватность, между национальным регулированием и глобальным характером сети). Анализ возможных краткосрочных и долгосрочных последствий для различных групп, включая научное сообщество.

- **Заключение (1-1.5 стр.):** Обобщающие выводы по результатам анализа. Сформулированная авторская позиция по проблеме. Практические рекомендации или предложения по разрешению/смягчению выявленных противоречий (на уровне личной практики исследователя, институциональных мер или публичной политики).
- **Список использованных источников:** Корректное оформление нормативно-правовых актов, научной литературы, материалов СМИ и интернет-ресурсов.

Примерные темы эссе:

1. Цифровая архивация личных дневников эпохи позднего СССР: правовые риски и этические дилеммы.
2. Феномен «исторического» deepfake: угроза доказательной базе исторической науки или новый инструмент популяризации?
3. Платформы краудсорсинга исторических данных (типа «Прожито»): анализ модели информационной безопасности и прав пользователей.
4. Регулирование социальных сетей как арены «войн памяти»: сравнительный анализ подходов РФ и ЕС.
5. Большие данные и биографические исследования: где грань между научным открытием и нарушением информационной приватности умерших?

Критерии оценки: глубина и самостоятельность анализа; корректность применения правовых норм и теоретических концепций; логичность и структурированность изложения; убедительность аргументации и выводов; грамотность и соблюдение академических стандартов оформления.

Объем эссе: 10-12 тыс. знаков (с пробелами).

9.3 Методические указания для обучающихся по освоению дисциплины

Курс «Информационная безопасность, информационный суверенитет: правовые и социальные аспекты» носит междисциплинарный характер и требует от студентов активной работы по синтезу знаний из разных областей.

Лекции задают концептуальную рамку, вводят ключевые термины, теории и правовые конструкции. Посещение лекций и внимательное конспектирование необходимы для формирования целостного понимания предмета.

Семинары являются ключевой площадкой для осмысления и применения полученных знаний. Успешная подготовка к семинару предполагает:

1. **Внимательное изучение обязательных материалов,** указанных в плане занятия (статьи, тексты законов, кейсы).
2. **Активную мыслительную работу:** не просто прочтение, а критическое осмысление, подготовка вопросов и собственных тезисов для дискуссии.
3. **Применение знаний на практике:** выполнение предложенных аналитических заданий, участие в ролевых играх и обсуждениях.

Самостоятельная работа:

1. **Отслеживание актуальности:** Сфера ИБ и цифрового права стремительно меняется. Рекомендуется следить за новостями (через авторитетные издания), за обновлениями законодательства и решениями судов по резонансным кейсам.
2. **Работа с первоисточниками:** Не ограничивайтесь пересказом учебных материалов. Учитесь самостоятельно находить и анализировать тексты законов, судебные решения, официальные отчеты и стратегические документы.

3. **Формирование личной позиции:** Курс затрагивает множество дискуссионных и этически сложных вопросов. Ваша задача – не просто запомнить точки зрения, а на основе фактов и аргументов сформировать собственную обоснованную позицию.
4. **Подготовка итогового эссе:** Начните думать над темой заранее. Постепенно собирайте материал, анализируйте возможные кейсы. Используйте консультации с преподавателем для уточнения формулировки проблемы и структуры работы.

Контроль знаний осуществляется непрерывно: через оценку активности и качества анализа на семинарах, выполнение промежуточных заданий и защиту итогового аналитического эссе. Наибольший вес имеет именно способность к комплексному, критическому и аргументированному анализу проблемных ситуаций.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Цель дисциплины «Информационная безопасность, информационный суверенитет: правовые и социальные аспекты»: сформировать у студентов-гуманитариев целостное понимание современных вызовов и угроз в цифровой среде, правовых механизмов их регулирования, а также социально-философских оснований концепций информационной безопасности и суверенитета, необходимых для критического анализа цифрового пространства и выработки стратегий профессиональной деятельности в условиях цифровой трансформации исторической науки.

Задачи дисциплины:

- Раскрыть сущность и многогранность понятий «информационная безопасность» и «информационный суверенитет» в междисциплинарной перспективе (технической, правовой, социально-гуманитарной).
- Изучить основные виды угроз информационной безопасности (кибератаки, дезинформация, манипуляция сознанием, утечки данных) и их потенциальное влияние на общество, историческую память и научные исследования.
- Сформировать представление об основах российского и международного права в сфере информационной безопасности, защиты персональных данных, интеллектуальной собственности и регулирования цифрового пространства.
- Проанализировать социальные, этические и политические аспекты информационного суверенитета, цифрового неравенства, свободы информации и цензуры в глобальном и национальном контекстах.
- Развить навыки критической оценки информационных угроз, анализа правовых кейсов и разработки базовых рекомендаций по обеспечению информационной безопасности в профессиональной деятельности историка.

В результате освоения дисциплины обучающийся должен:

Знать:

- основные концепции и методологии анализа цифрового общества, ключевые социальные теории, объясняющие природу информационных угроз и манипуляций;
- философские основания дискуссий о свободе информации, приватности и суверенитете в цифровую эпоху;
- базовые технические принципы функционирования ключевых элементов информационного пространства;
- систему российского законодательства в области информационной безопасности (ФЗ-149, ФЗ-152, ФЗ-187 и др.) и основы международного права, регулирующего киберпространство.

Уметь:

- выявлять и систематизировать различные типы угроз информационной безопасности в конкретных профессиональных и общественных контекстах;
- анализировать комплексные проблемные ситуации на стыке технологий, права и социума, формулировать научно обоснованные гипотезы и разрабатывать стратегические рекомендации;

- анализировать, как технологические особенности цифровых платформ формируют информационные потоки и влияют на общественное мнение и историческое сознание;
- применять знание правовых норм для оценки законности действий различных акторов в информационном пространстве и оценивать риски, связанные с обработкой данных в исследовательской работе.

Владеть:

- методологией системного анализа сложных социотехнических систем и навыками критической оценки источников информации;
- техниками сценарного прогнозирования для оценки социальных последствий технологических решений;
- навыками поиска и анализа актуальных нормативно-правовых актов в сфере ИБ;
- базовой терминологией в области кибербезопасности и цифрового права для профессиональной коммуникации;
- методикой составления карты стейкхолдеров в ситуациях, связанных с информационным суверенитетом.

Дисциплина ориентирована на формирование у будущих специалистов в области истории и цифровых гуманитарных наук критического, ответственного и стратегического подхода к работе в современном цифровом мире, где информация является одновременно объектом исследования, инструментом работы и полем острых правовых и социальных конфликтов.