МИНОБРНАУКИ РОССИИ

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

ИСТОРИКО-АРХИВНЫЙ ИНСТИТУТ
ФАКУЛЬТЕТ МЕЖДКНАРОДНЫХ ОТНОШЕНИЙ, ПОЛИТОЛОГИИ И ЗАРУБЕЖНОГО РЕГИОНОВЕДЕНИЯ

Кафедра международной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ЗАЩИТА ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ РЕСУРСОВ И СИСТЕМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

41.03.05 Международные отношения
Код и наименование направления подготовки/специальности

Международная безопасность: экспертиза и прогнозирование
Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2025

Информационная безопасность: защита информации и обеспечение безопасности электронных ресурсов и систем
Рабочая программа дисциплины

Составитель:
канд.филол.наук, доцент И.Ю. Бережанская

УТВЕРЖДЕНО
Протокол заседания кафедры международной безопасности
№ 4 от 12.12.2024

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – сформировать у студентов целостные знания об основах информационной безопасности, методах и способах защиты информации, обеспечении кибербезопасности. Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности. При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

Задачи дисциплины:

- - ознакомить учащихся с понятием «информационная безопасность» и различными трактовками в отечественной науке и за рубежом;
- - выявить особенности методов защиты информации;
- - обратить внимание на схожее и различное в способах защиты информации в России и в ряде иностранных государств;
- - развить у студентов умение работать с информационными ресурсами, посвященными изучаемой тематике;
- - дать полное представление об обеспечении безопасности электронных ресурсов и систем;
- - достигнуть творческого осмысления изучаемого материала, на основе полученных знаний, выработка учащимися собственного личностного видения процессов.

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

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-1. Способен самостоятельно работать с документами, научной литературой, материалами средств массовой информации, докладами экспертно-аналитических центров, базами данных, в том числе на иностранных языках	ПК-1.1. Знает труды ведущих отечественных и зарубежных экспертов по проблематике исследования и свободно ориентируется в документах, научной и периодической литературе, докладах, базах данных, в том числе на иностранном (-ых) языке(-ах).	Знать: основные российские и зарубежные источники и литературу по вопросу информационной безопасности. Уметь: анализировать необходимые источники и литературу, выявлять наиболее авторитетных авторов, делать выводы на основе

		изученного материала. Владеть: аналитическими навыками исследования проблемного поля в рамках исследуемой тематики.
ПК-5. Способен решать научные задачи, использовать методологию, обосновывать научную новизну и практическую значимость исследуемой проблематики в широком международном контексте	ПК-5.1. Обосновывает актуальность исследования, определяет объект и предмет исследования, формулирует научную проблему и/или гипотезу исследования.	Знать: методики исследования в изучаемом вопросе, основные современные точки зрения и проблемные аспекты. Уметь: определять главные параметры исследования и ориентиры, влияющие на них. Владеть: навыками определения научной проблемы или гипотезы по исследуемому вопросу.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность: защита информации и обеспечение безопасности электронных ресурсов и систем» относится к части, формируемой участниками образовательных отношений блока элективных дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Введение в профессию», «История международных отношений», «Методология исследований в области международной безопасности», «Информационная безопасность», «Международная безопасность».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: «Теория международных отношений», «Национальная, государственная и общественная безопасность России», «Противодействие международному терроризму и сепаратизму», а также прохождения производственной практики.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 5 з.е., 180 академических часов.

Семестр	Тип учебных занятий	Количество часов
4	Лекции	**22**
4	Семинары	**20**
	Всего:	**42**

Объем дисциплины в форме самостоятельной работы обучающихся составляет 118 академических часов.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1.	**Введение в информационную безопасность**	В разделе рассматривается термины, относящиеся к вопросам информационной безопасности, основные понятия, связанные с изучением вопроса, модели информационной безопасности, а также виды защищаемой информации
2.	**Правовое обеспечение информационной безопасности**	Раздел посвящен рассмотрению и анализу основных нормативно-правовых актов в области информационной безопасности. Особое внимание уделено правовым особенностям обеспечения безопасности конфиденциальной информации и государственной тайны
3.	**Технические средства и методы защиты информации**	В разделе анализируется проблематика инженерной защиты объектов, а также защиты информации от утечки по техническим каналам
4.	**Программно-аппаратные средства и методы обеспечения информационной безопасности**	Раздел посвящен рассмотрению основных видов сетевых и компьютерных угроз, отдельно анализируются средства и методы защиты от сетевых компьютерных угроз
5.	**Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности**	В разделе освещены вопросы использования баз данных для нахождения и изучения нормативных документов в области информационной безопасности
6.	**Обеспечение безопасности электронных ресурсов и систем**	В разделе рассматриваются различные настройки инструментов антивирусной защиты информации, иные технические средства
7.	**Кибербезопасность и кибертерроризм**	В разделе раскрываются вопросы теоретической концепции и современных характеристик понятия «кибербезопасность»; различие и сходство методик обеспечения кибербезопасности в России и за рубежом
8.	**Международное сотрудничество по обеспечению информационной безопасности**	В разделе рассматривается переговорный процесс и международное сотрудничество в области обеспечения как информационной, так и кибербезопасности

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

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: - опрос - тестирование (темы 1-4) - эссе	 4 балла 10 баллов 10 баллов	 40 баллов 10 баллов 10 баллов
Промежуточная аттестация Экзамен по билетам		40 баллов
Итого за семестр (дисциплину) Экзамен		100 баллов

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

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

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной,

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетвори-тельно»/ «зачтено (удовлетвори-тельно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворите льно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляется обучающемуся с

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		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

Примерный перечень вопросов для опроса на семинаре
(ПК-1.1., ПК-5.1.)

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

Критерии оценки опроса:

- **оценка «неудовлетворительно» (0 баллов)** ставится в том случае, если либо фактически не выполнены задания, нет демонстрации общей эрудиции и знаний лекционного материала;
- **оценка «удовлетворительно» (2 балла)** ставится, если ответы на задания неполные, есть ошибки, нет хорошей структуры ответа;
- **оценка «хорошо» (3 балла)** выставляется в том случае, если даны довольно полные ответы на задания, но допущены неточности, есть отдельные ошибки; нарушена структура ответа;
- **оценка «отлично» (4 балла)** выставляется студенту (за один опрос), если он дал исчерпывающие ответы на задания; ответы хорошо и логично структурированы.

Баллы суммируются.
Максимум – 40 баллов.

Примерный перечень вопросов для тестирования
(ПК-1.1., ПК-5.1.)

1. Сколько видов электронной подписи существует согласно Российскому законодательству?
   а) 2;
   б) 4;
   в) 1;
   г) 3.

2. Симметричное шифрование – это шифрование, в котором для зашифрования и расшифрования используется?
   а) два ключа;
   б) один ключ;
   в) три ключа;
   г) все ответы правильные.

3. Каким законом в Российской Федерации регламентируется процесс обработки и защиты персональных данных?
a) 1-ФЗ;
b) 97-ФЗ;
c) 137-ФЗ;
d) 152-ФЗ.

4. Кто имеет право выдавать сертификаты усиленной квалифицированной электронной подписи?

a) аккредитованный удостоверяющий центр;
b) организация, имеющая лицензию на деятельность по технической защите конфиденциальной информации;
c) любой удостоверяющий центр;
d) организация, имеющая лицензию на деятельность по техническому обслуживанию, модернизации и распространению шифровальных средств.

1. Что не относится к сведениям конфиденциального характера?
a) персональные данные;
b) сведения о сущности изобретения;
c) сведения, составляющие тайну следствия;
d) сведения о задолженности работодателей по выплате заработной платы и социальным выплатам.

Критерии оценки теста:

Оценка выставляется в виде суммы баллов. За правильно выполненное задание тестируемый получает максимальное количество баллов (**1 балл**), предусмотренное для этого задания, за неправильно выполненное – **0 баллов**.
После прохождения теста суммируются результаты выполнения всех заданий для выставления общей оценки за тест (**максимум – 10 баллов**).

Примерная тематика эссе
(ПК-1.1.)

1. Правовой режим защиты государственной тайны.
2. Защита интеллектуальной собственности средствами патентного и авторского права.
3. Особенности развития методов обеспечения кибербезопасности.
4. Кибертерроризм как новая угроза международной безопасности.

Критерии оценки эссе:

- **оценка «отлично» (10-8 баллов)** выставляется студенту, если он дал исчерпывающие ответы на задания; ответы хорошо и логично структурированы, написаны хорошим научным языком, грамотно;

- **оценка «хорошо» (7-5 баллов)** выставляется в том случае, если даны довольно полные ответы на задания, но допущены неточности, есть отдельные ошибки; нарушена структура ответа;
- оценка **«удовлетворительно» (4-2 балла)** ставится, если ответы на задания неполные, есть ошибки; написано небрежно, нет хорошей структуры ответа;
- оценка **«неудовлетворительно» (1-0 баллов)** ставится в том случае, если либо фактически не выполнены задания, либо нет демонстрации общей эрудиции и знаний лекционного материала.

Примерный список вопросов к экзамену по билетам

(ПК-1.1., ПК-5.1.)

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информации.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информации.
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
19. Симметричные шифры.
20. Ассиметричные шифры.
21. Криптографические протоколы.
22. Криптографические хеш-функции.
23. Электронная подпись.
24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.
28. Киберпреступность.
29. Кибертерроризм.
30. Способы и методы обеспечения безопасности электронных ресурсов и систем.

Критерии оценки экзамена по билетам:

При проведении промежуточной аттестации в виде экзамена студент должен ответить на 2 вопроса.

При оценивании ответа на вопрос учитывается:

- **оценка «неудовлетворительно» (6-1 балл)** ставится в том случае, если знание материала носит фрагментарный характер, наличие грубых ошибок в ответе;
- **оценка «удовлетворительно» (10-7 баллов)** выставляется, если материал освоен частично, допущено не более двух-трех недочетов;
- **оценка «хорошо» (14-11 баллов)** выставляется в том случае, если материал освоен почти полностью, допущено не более одного-двух недочетов, но обучающийся смог бы их исправить самостоятельно;
- **оценка «отлично» (20-15 баллов)** выставляется студенту, если материал освоен полностью, ответ построен по собственному плану.

После ответа на 2 вопроса баллы суммируются для выставления итоговой оценки за экзамен по билетам (**максимум – 40 баллов**).

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Литература
Основная

Источники:

1. Конституция Российской Федерации.
2. Уголовный кодекс Российской Федерации.
3. Федеральный закон № 149-ФЗ от 27.07.2006 (включая изменения и дополнения) «Об информации, информационных технологиях и защите информации».
4. Федеральный закон № 125-ФЗ от 22.10.2004 (включая изменения и дополнения) «Об архивном деле в Российской Федерации».
5. Федеральный закон № 128-ФЗ от 8.08.2001 «О лицензировании отдельных видов деятельности».
6. Федеральный закон № 152-ФЗ от 27.07.2006 (включая изменения и дополнения) «О персональных данных».
7. Федеральный закон № 85-ФЗ от 4.07.1996 «Об участии в международном информационном обмене».

Учебная:

1. Зенков, А.В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. – М.: Издательство Юрайт, 2022. – 104 с. – URL: https://urait.ru/book/informacionnaya-bezopasnost-i-zaschita-informacii-497002

2. Суворова, Г.М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. – М.: Издательство Юрайт, 2022. – 253 с. – URL: https://urait.ru/book/informacionnaya-bezopasnost-496741

3. Чернова, Е.В. Информационная безопасность человека: учебное пособие для вузов / Е. В. Чернова. – 2-е изд., испр. и доп. – М.: Издательство Юрайт, 2022. – 243 с. – URL: https://urait.ru/book/informacionnaya-bezopasnost-cheloveka-495922

Дополнительная

1. Интернет-библиотека русскоязычных СМИ Public.ru http://www. public.ru/
2. Научная электронная библиотека (НЭБ) http://elibrary.ru/
3. Университетская библиотека online http://www.biblioclub.ru/
4. ЭБС znanium.com издательства «ИНФРА-М» http://www.znanium.com/
5. Электронно-библиотечная система РУКОНТ http://rucont.ru/

6. Электронно-библиотечная система BOOK.ru http://www.book.ru/
7. Электронно-библиотечная система IPRbooks http://www.iprbookshop.ru/

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

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

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые компьютером и проектором для демонстрации учебных материалов.

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

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

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

- для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей.

Промежуточная аттестация может проводиться в несколько этапов.

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

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

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

- для слепых и слабовидящих:
- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.
- для глухих и слабослышащих:
- в печатной форме;
- в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата:
- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

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

- для слепых и слабовидящих:
  - устройством для сканирования и чтения с камерой SARA CE;
  - дисплеем Брайля PAC Mate 20;
  - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
  - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
  - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
  - передвижными, регулируемыми эргономическими партами СИ-1;
  - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы семинарских занятий

Тема 1. (4 ч.) Введение в информационную безопасность.

Вопросы для обсуждения:

1. Перечислите основные угрозы информационной безопасности.
2. Какие существуют модели информационной безопасности?
3. Какие методы защиты информации выделяют?
4. Что такое правовые методы защиты информации?
5. Что такое организационные методы защиты информации?

Тема 2. (2 ч.) Правовое обеспечение информационной безопасности.

Вопросы для обсуждения:

1. Какие нормативные правовые акты регламентируют защиту информации?
2. В чем сходство и различие правового регулирования защиты информации в России и за рубежом?
3. В чем заключается обновление законодательной базы по защите информации?

4. Каковы нововведения в Европе?
5. Каковы перспективы изменений в законодательной базе?
6.

Тема 3. (2 ч.) Технические средства и методы защиты информации.

Вопросы для обсуждения:

1. Что такое технические методы защиты информации?
2. Что такое программно-аппаратные методы защиты информации?
3. Перечислите методы защиты информации от утечки по индук-ционному каналу.
4. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
5. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.

Тема 4. (2 ч.) Программно-аппаратные средства и методы обеспечения информационной безопасности.

Вопросы для обсуждения:

1. Для чего нужна программно-аппаратная защита информации?
2. Защита от НСД.
3. Как взламывается аппаратно-программная защита и как избежать взлома?
4. Электронные ключи.

Тема 5. (2 ч.) Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.

Вопросы для обсуждения:

1. Каковы основные принципы отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации?
2. Каковы меры ответственности за нарушение правил защиты информации?
3. Назовите технико-математические решения вопросов организационно-правового обеспечения защиты информации?
4. Каков порядок разрешения спорных и конфликтных ситуаций по вопросам защиты информации?

Тема 6. (2 ч.) Обеспечение безопасности электронных ресурсов и систем.

Вопросы для обсуждения:

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?

Тема 7. (2 ч.) Кибербезопасность и кибертерроризм.

Вопросы для обсуждения:

1. Кибербезопасность в системе международной безопасности.
2. Кибертерроризм как новая угроза международной безопасности.
3. Соотношение безопасности личности, общества и государства.
4. Виды защищаемой электронной информации.
5. Способы и методы противостояния киберпреступлениям.

Тема 8. (4 ч.) Международное сотрудничество по обеспечению информационной безопасности.

Вопросы для обсуждения:

1. Информационная война, методы и средства её ведения.

2. Информационная безопасность и информационное противоборство.
3. Методы нарушения конфиденциальности, целостности и доступности информации.
4. Основные направления обеспечения информационной безопасности объектов информационной сферы страны в условиях информационной войны.

9.2. Методические рекомендации по написанию письменных работ

Методические рекомендации по написанию эссе

Требования к оформлению работы:
Объем работы – не больше одного печатного листа формата А4.
Оригинальность работы должна быть не ниже 90%.

- **Начало эссе**

1. Заголовок эссе работы (указывается прописными буквами, шрифтом Times New Roman 14, полужирный, полуторный, выравнивается по центру).
2. ФИО автора (сначала указываются имя и отечество автора, затем фамилия). Шрифт Times New Roman 12, полужирный, межстрочный интервал одинарный, выравнивание по центру. На следующей строке – курс и порядковый номер группы.

- **Основной текст работы**

Основной текст оформляется шрифтом Times New Roman 14, обычный, межстрочный интервал полуторный, выравнивается по ширине. Каждый абзац начинается с красной строки. Отступ 1,25 см. Не ставятся точки в конце заголовка статьи, разделов, названий рисунков и таблиц. Эссе должно начинаться с введения, в котором следует отразить постановку задачи работы. В основном тексте эссе дается анализ проблемы, разъясняются полученные утверждения и результаты. Заключение должно содержать обсуждение полученных результатов.

- **Конец эссе**

Список источников и литературы приводится в конце работы. Ссылки на источники и литературу являются обязательным атрибутом эссе. Список литературы оформляется в виде концевых сносок.
Выполненная работа должна соответствовать вышеуказанным требованиям.

9.3. Иные материалы

Самостоятельная работа нацелена на расширение теоретических и фактических знаний, когнитивных и практических умений на основе поиска и анализа информации, а также изучения студентами историографической и источниковедческой базы курса при подготовке к семинарским занятиям, текущему контролю и промежуточной аттестации.

Самостоятельная работа может выполняться студентом в читальном зале библиотеки, в компьютерных классах, а также в домашних условиях.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность: защита информации и обеспечение безопасности электронных ресурсов и систем» реализуется на факультете международных отношений, политологии и зарубежного регионоведения кафедрой международной безопасности.

Цель дисциплины – сформировать у студентов целостные знания об основах информационной безопасности, методах и способах защиты информации, обеспечении кибербезопасности. Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности. При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

Задачи дисциплины:

- - ознакомить учащихся с понятием «информационная безопасность» и различными трактовками в отечественной науке и за рубежом;
- - выявить особенности методов защиты информации;
- - обратить внимание на схожее и различное в способах защиты информации в России и в ряде иностранных государств;
- - развить у студентов умение работать с информационными ресурсами, посвященными изучаемой тематике;
- - дать полное представление об обеспечении безопасности электронных ресурсов и систем;
- - достигнуть творческого осмысления изучаемого материала, на основе полученных знаний, выработка учащимися собственного личностного видения процессов.

Дисциплина направлена на формирование следующих компетенций:

ПК-1 – способен самостоятельно работать с документами, научной литературой, материалами средств массовой информации, докладами экспертно-аналитических центров, базами данных, в том числе на иностранных языках;

ПК-5 – способен решать научные задачи, использовать методологию, обосновывать научную новизну и практическую значимость исследуемой проблематики в широком международном контексте.

В результате освоения дисциплины обучающийся должен:

Знать:

- основные российские и зарубежные источники и литературу по вопросу информационной безопасности;

- методики исследования в изучаемом вопросе, основные современные точки зрения и проблемные аспекты.

Уметь:

- анализировать необходимые источники и литературу, выявлять наиболее авторитетных авторов, делать выводы на основе изученного материала;
- определять главные параметры исследования и ориентиры, влияющие на них.

Владеть:

- аналитическими навыками исследования проблемного поля в рамках исследуемой тематики;
- навыками определения научной проблемы или гипотезы по исследуемому вопросу.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц.