



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
«Б1.В.ДВ.01.02 РАЗРАБОТКА ПОДСИСТЕМЫ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ»**

Уровень высшего образования: магистратура

Направление подготовки: 10.04.01 Информационная безопасность

Направленность(профиль) подготовки: Защита информации в геоинформационных системах
и системах сбора пространственных данных

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 2 года

Объем:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2024

Разработчики:

Преподаватель кафедры Информационно-измерительных систем
Сутягин Д. Д.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки от 26.11.2020 № 1455

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

Содержание

1. Цель и задачи освоения дисциплины (модуля)
2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы
3. Место дисциплины в структуре ОП
4. Объем дисциплины и виды учебной работы
5. Содержание дисциплины
 - 5.1. Разделы, темы дисциплины и виды занятий
 - 5.2. Содержание разделов, тем дисциплины и формы текущего контроля
6. Оценочные материалы текущего контроля
7. Оценочные материалы промежуточной аттестации
8. Порядок проведения промежуточной аттестации
9. Материально-техническое и учебно-методическое обеспечение дисциплины
 - 9.1. Перечень основной и дополнительной учебной литературы
 - 9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
 - 9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
 - 9.4. Оборудование и технические средства обучения
10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование у обучающихся навыков для проектирования, внедрения и обслуживания защищенных веб-приложений.

Задачи изучения дисциплины:

- Изучение методов защиты веб-приложений от э критических угроз безопасности.;
- Изучение методов внедрения безопасного управления сеансами для предотвращения таких атак, как перехват сеанса.;
- Развертывание веб-приложений в безопасной среде и текущем обслуживании для обеспечения безопасности веб-приложений..

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-3 Способен разрабатывать проектные решения по защите информации автоматизированных систем (в том числе в геоинформационных системах)

ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности

Знать:

ПК-3.1/Зн1 нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности

ПК-3.1/Зн2 методы безопасности веб-приложения от критических угроз безопасности

Уметь:

ПК-3.1/Ум1 классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности

ПК-3.1/Ум2 выявлять и устранять потенциальные угрозы безопасности в веб-приложениях

Владеть:

ПК-3.1/Нв1 методами анализа и оценки информации на предмет ее соответствия критериям отнесения к различным видам тайны и степеням конфиденциальности

ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты

Знать:

ПК-3.2/Зн1 нормативные и методические документы, регламентирующие классификацию субъектов и объектов доступа

ПК-3.2/Зн2 принципы и методы организационной защиты информации

ПК-3.2/Зн3 методы атаки и различные методы предотвращения атак

Уметь:

ПК-3.2/Ум1 определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации

Владеть:

ПК-3.2/Нв1 навыками работы с системами управления доступом и средствами контроля доступа

ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации

Знать:

ПК-3.3/Зн1 регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем

Уметь:

ПК-3.3/Ум1 разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем

ПК-3.3/Ум2 развертывать веб-приложения в безопасной среде и поддерживать безопасность веб-приложений

Владеть:

ПК-3.3/Нв1 навыками разработки проектов нормативных документов, регламентирующих работу по защите информации в организации

ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

Знать:

ПК-3.4/Зн1 принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

ПК-3.4/Зн2 стек протоколов TCP/IP и модель OSI

ПК-3.4/Зн3 технологии проектирования и построения защищенных информационных систем

Уметь:

ПК-3.4/Ум1 анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации

Владеть:

ПК-3.4/Нв1 навыками проектирования и построения локальных и глобальных компьютерных сетей с использованием современных технологий и оборудования

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.ДВ.01.02 «Разработка подсистемы защиты веб-приложений» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 1.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
1 семестр	144	4	68	76	Зачет
Всего	144	4	68	76	

5. Содержание дисциплины (модуля)
5.1. Разделы, темы дисциплины и виды занятий
(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Практические занятия	Самостоятельная работа	Планируемые результаты с обучения, соотнесенные с результатами освоения программы
Раздел 1. Введение в безопасность веб-приложений	20	12	8	ПК-3.1
Тема 1.1. Введение в безопасность веб-приложений: настройка среды разработки	20	12	8	
Раздел 2. Проверка ввода и очистка данных	16	8	8	ПК-3.1 ПК-3.2
Тема 2.1. Проверка ввода и очистка данных: реализация проверки ввода и очистка в веб-приложении	16	8	8	
Раздел 3. Аутентификация и контроль доступа	16	8	8	ПК-3.2
Тема 3.1. Аутентификация и контроль доступа: реализация аутентификации и контроля доступа в веб-приложении	16	8	8	
Раздел 4. Управление сеансом	18	8	10	ПК-3.3 ПК-3.4
Тема 4.1. Управление сеансом: реализация управления сеансом в веб-приложении	18	8	10	
Раздел 5. Межсайтовый скриптинг (XSS)	18	8	10	ПК-3.4
Тема 5.1. Межсайтовый скриптинг (XSS): предотвращение и смягчение последствий XSS-атак	18	8	10	
Раздел 6. Межсайтовая подделка запросов (CSRF)	18	8	10	ПК-3.4
Тема 6.1. Подделка межсайтовых запросов (CSRF): предотвращение и смягчение последствий CSRF-атак	18	8	10	
Раздел 7. SQL Injection	18	8	10	ПК-3.1 ПК-3.2 ПК-3.4
Тема 7.1. Внедрение SQL: предотвращение и смягчение атак путем внедрения SQL	18	8	10	

Раздел 8. Развертывание и обслуживание	20	8	12	ПК-3.1 ПК-3.2
Тема 8.1. Развертывание и обслуживание: развертывание безопасного веб-приложения	20	8	12	ПК-3.3 ПК-3.4
Итого	144	68	76	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Введение в безопасность веб-приложений

Тема 1.1. Введение в безопасность веб-приложений: настройка среды разработки

Важность безопасности веб-приложений, распространенные типы атак, OWASP Top 10, матрица MITRE Att&ck, оценка рисков.

Раздел 2. Проверка ввода и очистка данных

Тема 2.1. Проверка ввода и очистка данных: реализация проверки ввода и очистки в веб-приложении

Проверка ввода, очистка данных, важность для безопасности веб-приложений. Fuzzing тестирование. OpenApi спецификация.

Раздел 3. Аутентификация и контроль доступа

Тема 3.1. Аутентификация и контроль доступа: реализация аутентификации и контроля доступа в веб-приложении

Аутентификация, контроль доступа, защита сеансов пользователей. JWT. OAuth. Keycloak. RBAC\ABAC, , политики паролей.

Раздел 4. Управление сеансом

Тема 4.1. Управление сеансом: реализация управления сеансом в веб-приложении

Управление сеансом, безопасное управление сеансом, предотвращение перехвата сеанса. Cookie. Библиотеки и инструменты для реализации механизмов безопасного управления сеансами.

Раздел 5. Межсайтовый скриптинг (XSS)

Тема 5.1. Межсайтовый скриптинг (XSS): предотвращение и смягчение последствий XSS-атак

XSS-атаки, методы предотвращения XSS-атак, инструменты эксплуатации XSS, инструменты автоматизации поиска XSS, экранирование и кодирование.

Раздел 6. Межсайтовая подделка запросов (CSRF)

Тема 6.1. Подделка межсайтовых запросов (CSRF): предотвращение и смягчение последствий CSRF-атак

CSRF-атаки, реализация защиты от CSRF. Шаблон токена синхронизатора. Фреймворки, с CSRF защитой. Библиотеки для интеграции защиты от CSRF.

Раздел 7. SQL Injection

Тема 7.1. Внедрение SQL: предотвращение и смягчение атак путем внедрения SQL

Атаки с внедрением SQL, методы предотвращения атак с внедрением SQL, параметризованные запросы. Инструменты для автоматизации поиска sqlinjection. Фреймворки, с SQLi защитой. Библиотеки для интеграции защиты от SQLi.

Раздел 8. Развертывание и обслуживание

Тема 8.1. Развертывание и обслуживание: развертывание безопасного веб-приложения

Развертывание веб-приложений в безопасной среде, текущее обслуживание для обеспечения безопасности, обновления безопасности, мониторинг. Тонкая детальная работа с docker. WAF. Ci\Cd DevSecOps.

Текущий контроль

Вид (форма) контроля
Тестирование

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Зачет, 1 семестр.

Зачет оценивается по следующей шкале:

- оценка «зачтено» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное

изложение материала; демонстрирует свободное применение теоретических знаний; а также автоматически, когда обучающийся за промежуточную аттестацию имеет оценки «отлично»;

- оценка «не зачтено» выставляется обучающемуся в случае наличия грубых ошибок при изложении ответа на основные вопросы программы, свидетельствующих о неправильном понимании предмета; при решении практических задач показано незнание способов их решения, материал изложен беспорядочно и неуверенно.

7. Оценочные материалы текущего контроля

Раздел 8. Развертывание и обслуживание

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 8.1. Развертывание и обслуживание: развертывание безопасного веб-приложения

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое безопасность веб-приложений?
 1. Практика защиты веб-приложений от несанкционированного доступа и вредоносных атак
 2. Практика защиты веб-серверов от несанкционированного доступа и вредоносных атак
 3. Практика защиты веб-сайтов от несанкционированного доступа и вредоносных атак
2. Почему важна безопасность веб-приложений?
 1. Для защиты конфиденциальности конфиденциальной информации, хранящейся в веб-приложении
 2. Обеспечить доступность веб-приложения для авторизованных пользователей
 3. Оба а и 2
3. Какие распространенные типы атак могут быть нацелены на веб-приложения?
 1. Атаки с использованием межсайтового скриптинга (XSS)
 2. Атаки SQL-инъекций
 3. Оба а и 2
4. Что такое Топ-10 OWASP?
 1. Список наиболее серьезных угроз безопасности, с которыми сталкиваются веб-сайты
 2. Список наиболее серьезных угроз безопасности, с которыми сталкиваются веб-серверы
 3. Список наиболее серьезных угроз безопасности, с которыми сталкиваются веб-приложения
5. Как вы можете защитить свое веб-приложение от угроз, перечисленных в Топ-10 OWASP?
 1. Путем реализации мер безопасности, таких как проверка ввода, очистка данных и безопасное управление сеансами
 2. Игнорируя OWASP Top 10 и надеясь, что ваше веб-приложение будет безопасным
 3. Применяя меры безопасности только для наиболее серьезных угроз
6. Что из нижеперечисленного не входит в десятку лучших OWASP?
 1. Атаки с использованием межсайтового скриптинга (XSS)
 2. Атаки с подделкой межсайтовых запросов (CSRF)
 3. DDoS-атаки
7. Что такое проверка ввода?
 1. Процесс проверки вводимых пользователем данных, чтобы убедиться, что они соответствуют заданным критериям
 2. Процесс дезинфекции вводимых пользователем данных для обеспечения их безопасного использования
 3. Процесс шифрования вводимых пользователем данных для защиты их от несанкционированного доступа
8. Почему важна проверка ввода?
 1. Для предотвращения вредоносных атак, таких как SQL-инъекция
 2. Для обеспечения доступности веб-приложения

3. Оба а и 2

9. Какие существуют методы очистки данных?

1. Проверка ввода
2. Экранирование пользовательского ввода
3. Оба а и 2

10. Что такое аутентификация?

1. Процесс проверки личности пользователя
2. Процесс предоставления доступа пользователю
3. Оба а и 2

11. Каково значение управления паролями для аутентификации?

1. Для предотвращения несанкционированного доступа к веб-приложению.
2. Для обеспечения доступности веб-приложения.
3. Оба

12. Что такое управление сессиями?

1. Процесс управления сессиями пользователей в веб-приложении
2. Процесс управления сеансами сервера в веб-приложении
3. Процесс управления сеансами базы данных в веб-приложении

13. Что такое перехват сеанса?

1. Тип атаки, при которой злоумышленник получает контроль над сеансом пользователя
2. Тип атаки, при которой злоумышленник получает контроль над сеансом сервера
3. Тип атаки, при которой злоумышленник получает контроль над сеансом базы данных

14. Каков наилучший способ предотвратить перехват сеанса?

1. С помощью зашифрованных файлов cookie
2. Используя идентификаторы сеанса в URL-адресе
3. Используя как зашифрованные файлы cookie, так и идентификаторы сеанса в URL-адресе

15. Что такое межсайтовый скриптинг (XSS)?

1. Тип атаки, при котором злоумышленник внедряет вредоносные скрипты на веб-страницу
2. Тип атаки, при котором злоумышленник использует уязвимости на веб-странице
3. Тип атаки, при которой злоумышленник крадет конфиденциальную информацию с веб-страницы

16. Какие существуют типы XSS-атак?

1. Сохраненные XSS и отраженные XSS
2. XSS на стороне клиента и XSS на стороне сервера
3. Ввод XSS и вывод XSS

17. Как лучше всего предотвратить XSS-атаки?

1. Проверая ввод пользователя
2. Путем шифрования конфиденциальной информации
3. Используя защищенную базу данных

18. Что такое подделка межсайтовых запросов (CSRF)?

1. Тип атаки, при которой злоумышленник обманом заставляет пользователя совершать непреднамеренные действия
2. Тип атаки, при котором злоумышленник использует уязвимости в веб-приложении
3. Тип атаки, при которой злоумышленник крадет конфиденциальную информацию из веб-приложения

19. Как работает CSRF-атака?

1. Путем внедрения вредоносных скриптов на веб-страницу
2. Заставляя пользователя совершать непреднамеренные действия
3. Используя уязвимости в веб-приложении

20. Каков наилучший способ предотвратить атаки CSRF?

1. Проверая ввод пользователя
2. Используя токены анти-CSRF
3. Используя как токены анти-CSRF, так и проверяя ввод пользователя

21. Что такое атака SQL Injection?

1. Атака, при которой злоумышленник внедряет вредоносный код в базу данных SQL веб-сайта
2. Атака, при которой злоумышленник отправляет вредоносный запрос на сервер веб-сайта
3. Атака, при которой злоумышленник использует уязвимости в коде веб-сайта

22. Какова цель атаки SQL Injection?

1. Чтобы украсть конфиденциальную информацию, хранящуюся в базе данных веб-сайта
2. Чтобы получить контроль над сервером веб-сайта
3. Чтобы вызвать отказ в обслуживании

23. Каков наилучший способ предотвратить атаки SQL Injection?

1. Использование брандмауэра
2. Дезинфекция пользовательского ввода
3. Шифрование конфиденциальной информации

24. Что подразумевается под «экранированием» пользовательского ввода?

1. Преобразование пользовательского ввода в другой формат
2. Замена символов в пользовательском вводе их эквивалентными кодами HTML
3. Добавление дополнительных символов к пользовательскому вводу, чтобы сделать его безопасным для использования в SQL-запросе

25. Какова цель развертывания веб-приложения?

1. Сделать приложение доступным для пользователей через Интернет
2. Чтобы протестировать приложение в реальной среде
3. Для оптимизации производительности приложения

26. Какова основная цель текущего обслуживания веб-приложения?

1. Чтобы приложение оставалось безопасным и функциональным
2. Для улучшения пользовательского интерфейса приложения
3. Чтобы уменьшить время загрузки приложения

27. Что подразумевается под «безопасной средой» для развертывания веб-приложения?

1. Физическое местоположение с контролируемым доступом
2. Виртуальная среда с надлежащими мерами безопасности
3. Место, где хранится приложение

28. Почему важно постоянно обновлять веб-приложение с помощью последних исправлений безопасности?

1. Чтобы злоумышленники не использовали известные уязвимости.
2. Для повышения производительности приложения.
3. Чтобы приложение соответствовало отраслевым стандартам.

8. Оценочные материалы промежуточной аттестации

1 семестр, Зачет

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Вопросы/Задания:

1. Что такое подсистема защиты веб-приложений и почему она важна?
2. Каковы общие угрозы для веб-приложений и как их можно смягчить?
3. Что такое межсайтовый скриптинг (XSS) и как его предотвратить?
4. Что такое SQL-инъекция и как ее предотвратить?
5. Что такое подделка межсайтовых запросов (CSRF) и как ее предотвратить?

6. Что такое неправильная настройка безопасности и как ее предотвратить?
7. Что такое слабая аутентификация и авторизация и как их предотвратить?
8. Что такое нарушенный контроль доступа и как его предотвратить?
9. Что такое раскрытие конфиденциальных данных и как его можно предотвратить?
10. Что такое нарушенное управление сессией и как его предотвратить?
11. Что такое нарушение безопасности и как его обнаружить и предотвратить?
12. Какие существуют типы алгоритмов шифрования и как они работают?
13. Что такое SSL/TLS и как он обеспечивает безопасную связь через Интернет?
14. Что такое проект OWASP Top Ten и как его можно использовать для защиты веб-приложений?
15. Какова роль брандмауэров и систем обнаружения вторжений в безопасности веб-приложений?
16. Как можно проводить тестирование безопасности веб-приложений?
17. Какие существуют типы тестирования безопасности и чем они отличаются друг от друга?
18. Какова важность моделирования угроз в безопасности веб-приложений?
19. Какова роль ведения журнала безопасности и мониторинга в безопасности веб-приложений?
20. Каковы передовые методы обеспечения безопасности веб-приложений?
21. Как сделать веб-приложение более безопасным с помощью фреймворков и библиотек безопасности?
22. Какова роль проверки ввода в безопасности веб-приложений?
23. Какова важность методов безопасного кодирования для безопасности веб-приложений?
24. Как сделать веб-приложение более безопасным, используя лучшие практики и стандарты безопасности?
25. Какова важность регулярного обновления и исправления веб-приложений и базовых систем?
26. Какова роль образования и осведомленности в области безопасности веб-приложений?

27. Каковы этические и правовые последствия безопасности веб-приложений?
28. Как можно интегрировать безопасность веб-приложений в процесс разработки?
29. Какова роль тестирования на проникновение в безопасность веб-приложений?
30. Как можно повысить безопасность веб-приложений с помощью инструментов и служб безопасности?

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Галатенко В. А. Основы информационной безопасности: учебное пособие: учебное пособие / В. А. Галатенко. - Основы информационной безопасности - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 266 с. - 978-5-4497-3316-0. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/142285.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
2. Лапониная О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учебное пособие: учебное пособие / О. Р. Лапониная; под редакцией В. А. Сухомлина. - Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 605 с. - 978-5-4497-3470-9. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/142292.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «правовое обеспечение национальной безопасности»: учебник для студентов вузов, обучающихся по направлению подготовки «правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. - Основы информационной безопасности - Москва: ЮНИТИ-ДАНА, 2023. - 287 с. - 978-5-238-02857-6. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/141624.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. <https://www.iprbookshop.ru/> - IPR BOOKS
2. <https://www.elibrary.ru/> - НЭБ eLIBRARY
3. <https://rusneb.ru/> - Национальная электронная библиотека (НЭБ)

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения

(обновление производится по мере появления новых версий программы)

1. Microsoft Visual Studio;

Перечень информационно-справочных систем

(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Учебная аудитория

Маркерная доска - 0 шт.

Моноблок - 64 шт.

Проектор - 4 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется:

- Методическими рекомендациями по дисциплине;
- Методическими рекомендациями по организации самостоятельной работы студентов МИИГАиК;

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.