АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ИНСТИТУТ ЭКОНОМИКИ И УПРАВЛЕНИЯ В ПРОМЫШЛЕННОСТИ»

Экономический факультет

Кафедра Экономики

УТВЕРЖДАЮ
Ректор АНО ВО «Институт экономики и управления в промышленности»

_____Рябинин А.В.
«24» ноября 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

39.03.03 «Организация работы с молодежью»
(профиль – Государственное управление молодежной политикой)

Квалификация выпускника: бакалавр

Москва, 2025 г.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- формирование у студентов принципов информационной безопасности государства, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации

Краткое описание/аннотации дисциплины

В дисциплине осуществляется знакомство студентов с определением, классификацией и характеристиками информационной безопасности; с организационными и экономическими аспектами работы с информационными ресурсами и методами оценки эффективности их безопасности. Дисциплина даёт представление об особенностях информационной безопасности, сегментах и участниках информационного рынка, особенностях формирования безопасности информации. В дисциплине рассматриваются основные технологические принципы безопасности мировых информационных ресурсов на основе глобальной сети Internet и основные механизмы обеспечения безопасности ресурсов Internet.

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Компетенции обучающегося, формируемые в результате освоения данной дисциплины:

ОПК-1 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

3.ТЕМАТИЧЕСКИЙ ПЛАН ДИСЦИПЛИНЫ

Семестр: 3

Форма обучения: очная

Аттестация: зачет

№	Темы (разделы) дисциплины	Виды аудиторной работы (в ак.час.)			Итого аудиторных ак.часов по теме
		Лекции	Практические занятия	Самостоятельная работа	
1	Основные составляющие информационной безопасности. Понятие «информационная безопасность». Проблема информационной безопасности общества	2	4	4	10
2	Угрозы информационной безопасности Основные определения и критерии классификации угроз. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.	2	4	4	10

3	Вредоносное программное обеспечение. Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Характеристики «вирусоподобных» программ.	2	4	4	10
4	Антивирусные программы.	3	4	4	11
5	Профилактика компьютерных вирусов и обнаружение неизвестного вируса.	3	4	4	11
6	Основы международного законодательства в области информационной безопасности и защиты информации. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности.	3	4	4	11
7	Стандарты и спецификации в области информационной безопасности.	3	4	4	11
8	Административный уровень обеспечения информационной безопасности: цели, задачи, содержание, разработка политики информационной безопасности.	3	4	4	11
9	Управление рисками. Процедурный уровень информационной безопасности. Основные программно-технические меры.	3	4	4	11
	Итого:	24	36	36	96

4. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для изучения дисциплины используются различные образовательные технологии:

1. Интерактивные лекции, создающие в аудитории атмосферу доверительного и взаимоуважительного диалога студентов с преподавателем.

2. Практические занятия, на которых в атмосфере доверительного и взаимоуважительного диалога студентов между собой и преподавателем обсуждаются вопросы лекций и домашних заданий; делаются доклады, устное реферирование предложенной преподавателем литературы; проводятся дискуссии, групповая работа, выполняются контрольные работы.

3. Самостоятельная работа студентов, включающая усвоение теоретического материала, чтение и подготовку конспектов первоисточников, подготовку к практическим занятиям, подготовку докладов и сообщений, выполнение творческих заданий, контрольных работ (рефератов), контрольных работ, тезисов, статей, работу с электронным учебно-методическим комплексом, подготовку к текущему контролю знаний и к промежуточной аттестации – экзамену.

4. Тестирование по отдельным темам дисциплины, по модулям программы.

5. Научно-исследовательская работа студентов (НИРС), включающая занятия студентов в студенческом научном обществе, участие в конференциях, олимпиадах.

6. Консультирование студентов по вопросам учебного материала,

подготовки тезисов, статей, докладов.

7. При реализации образовательной программы с применением дистанционных образовательных технологий и электронного обучения:

- состав видов контактной работы по дисциплине (модулю), при необходимости, может быть откорректирован в направлении снижения доли занятий лекционного типа и соответствующего увеличения доли консультаций (групповых или индивидуальных) или иных видов контактной работы;

- информационной основой проведения учебных занятий, а также организации самостоятельной работы обучающихся по дисциплине (модулю) являются представленные в электронном виде методические, оценочные и иные материалы, размещенные в электронной информационно-образовательной среде (ЭИОС) института, в электронных библиотечных системах и открытых Интернет-ресурсах;

- взаимодействие обучающихся и педагогических работников осуществляется с применением ЭИОС института и других информационно-коммуникационных технологий (видео-конференц-связь, облачные технологии и сервисы, др.);

- соотношение контактной и самостоятельной работы по дисциплине (модулю) может быть изменено в сторону увеличения последней, в том числе самостоятельного изучения теоретического материала.

-

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Контрольные вопросы и задания для проведения промежуточной аттестации по итогам освоения дисциплины

Задача №1: Выбор метода шифрования. Допустим, вам необходимо защитить небольшой объем важной информации средствами свободного программного обеспечения. Среди возможных способов шифрования выбрана программа Веракрипт (Veracrypt). Почему Веракрипт предпочтительнее стандартного архиватора ZIP с функцией шифрования?

Решение: Веракрипт обеспечивает значительно большую степень защиты благодаря использованию мощных алгоритмов шифрования (AES, Twofish, Serpent), многократному прохождению процесса шифрования и поддержке скрытых контейнеров. Архиватор ZIP использует упрощённый метод шифрования, который легко взломать даже простыми методами перебора ключей.

Задача №2: Определение типов атак. Предположим, злоумышленники используют следующую технику атаки: они создают поддельный веб-интерфейс известного банка, заставляя пользователей вводить личные данные (логин, пароль, номер карты). Как называется такая атака?

Решение: Эта техника называется Фишинг (Phishing). Фишинг — это вид социальной инженерии, при которой мошенники обманом заставляют жертву раскрыть личную информацию путём подделывания доверительных ресурсов (сайтов банков, компаний и т.д.).

Задача №3: Методы аутентификации. Вы собираетесь внедрить двухфакторную аутентификацию для входа в личный кабинет сайта. Один из факторов — ввод

пароля. Второй фактор предлагается выбрать из следующих вариантов: отпечаток пальца, SMS-код, секретный вопрос. Какой вариант наилучшим образом повысит уровень безопасности аккаунта?
Решение: Самым безопасным вариантом второго фактора аутентификации является получение одноразового SMS-кода. Хотя биометрические методы вроде отпечатка пальца обеспечивают высокий уровень защиты, они менее распространены и сложнее интегрируются. Вопросы безопасности зачастую легко угадать или выяснить методом социального инжиниринга. SMS-код же поступает непосредственно на телефон владельца и требует физического владения устройством, что делает атаку намного сложнее.

Задача №4: Антивирусная защита. Почему использование бесплатного антивирусного сканера ClamAV считается хорошим решением для небольших организаций или частных лиц?
Решение: ClamAV является популярным открытым проектом с обширной базой известных вредоносных программ. Он распространяется бесплатно и предлагает эффективные механизмы выявления большинства распространенных видов угроз. Благодаря широкому сообществу разработчиков, база данных постоянно пополняется новыми сигнатурами. Его использование целесообразно там, где критична экономия средств, а требования к защите высоки.

Задача №5: Основы криптографии. Какой стандарт шифрования используется большинством программных средств и признан одним из самых надежных на сегодняшний день?
Решение: Стандарт шифрования, признанный мировым лидером надежности и производительности, — это AES (Advanced Encryption Standard). Этот алгоритм применяется в большинстве приложений и сертифицирован правительственными организациями многих стран мира. Другие распространенные стандарты, такие как DES или RC4, считаются устаревшими и недостаточно надежными.

Задача №6. Вам нужно отправить важную документацию клиенту по электронной почте. Но есть риск, что почта перехватывается третьими лицами. Чем зашифровать вложения, чтобы информация была доступна только получателю?
Решение: Можно использовать GnuPG (GNU Privacy Guard) — свободный аналог PGP-шифрования. Она обеспечит надежную защиту вложений и гарантирует, что расшифровать их сможет лишь тот, кому предназначается письмо.

Задача №7. Разработчику необходимо протестировать свое веб-приложение на наличие уязвимостей. Какой инструмент выбрать для этого?
Решение: Рекомендуется использовать OWASP ZAP (Zed Attack Proxy) — мощный и популярный инструмент с открытым исходным кодом, предназначенный для автоматического поиска уязвимостей веб-приложений.

Задача №8. Организации требуется убедиться, что передаваемые ей данные защищены от прослушивания в каналах связи. Какой метод шифрования наиболее

целесообразен?
Решение: Лучше всего использовать TLS (Transport Layer Security) — современный стандарт безопасного соединения, который защищает данные при передаче по сети. Он поддерживается всеми популярными браузерами и серверами и предоставляется бесплатно.

Задача №9. Компании нужен надежный инструмент для аудита уязвимостей внутренних серверов и рабочих станций. Какой бесплатный инструмент подойдет?
Решение: Эффективным средством для инвентаризации уязвимостей является Nessus Home Edition (для небольшого числа устройств) или OpenVAS — оба инструмента имеют открытые исходные коды и способны обнаружить большинство типовых проблем безопасности.

Задача №10. Вам необходимо организовать мониторинг сетевого трафика для выявления аномалий и потенциально опасных действий в сети предприятия. Какой инструмент использовать?
Решение: Свободный инструмент Wireshark прекрасно справится с задачей захвата и анализа сетевого трафика. Он обладает мощными возможностями фильтраций и способен распознавать различные типы сетевых протоколов и событий.

Задача №11. Молодёжная общественная организация проводит конкурс творческих работ в цифровом формате. Участников предупреждают о важности защиты авторских прав и предлагают загрузить файлы на специальный портал. Как участник конкурса может защитить своё творческое произведение от кражи и плагиата?
Решение: Участник конкурса может предварительно поставить водяной знак на художественное произведение, будь то рисунок, фотография или текст. Водяной знак может представлять собой прозрачную надпись с именем автора или специальным знаком копирайта, размещённую поверх произведения. Это простое действие существенно затрудняет незаконное использование чужого творчества.

Задача №12. Во время дистанционного образовательного мероприятия подросткам выдаются инструкции по проведению мастер-класса по компьютерной графике. Преподаватель опасается, что учащиеся случайно поделятся этими инструкциями в открытом доступе. Какие меры можно принять для минимизации риска распространения чувствительной информации?
Решение: Преподаватель может передать инструкцию в виде защищённого архива с паролем, известным только учащимся. Например, создав архив с помощью любого бесплатного инструмента, например, WinRAR или 7-Zip, преподаватель устанавливает сложный пароль и дополнительно предупреждает учащихся о недопустимости разглашения.

Задача №13. Старшеклассники проводят исследование по изучению предпочтений молодёжи в выборе профессий будущего. Они собирают анкетные данные онлайн. Как избежать утечки полученных сведений?
Решение: Анкетирование лучше проводить через специальные формы, интегрированные с системами хранения данных, такими как Google Формы или Яндекс.Формулы. Эти сервисы хранят собранные данные в зашифрованном виде и предоставляют доступ только администратору анкеты, минимизируя вероятность потери данных и несанкционированного доступа третьих лиц.

Задача №14. Учреждение дополнительного образования открывает группу молодых программистов, которым предстоит работа с открытыми исходниками и сторонними библиотеками. Руководителю необходимо объяснить ученикам, как минимизировать риски заражения вредоносным кодом при использовании публичных библиотек.
Решение: Руководитель объясняет ученикам важность проверок безопасности внешних зависимостей и рекомендует пользоваться специальными инструментами анализа зависимости, такими как OWASP Dependency Checker, позволяющий находить известные уязвимые библиотеки и предлагать альтернативы.

Задача №15. Молодежная команда создаёт благотворительное мероприятие и собирает добровольцев через регистрационную форму на своем сайте. Организаторы хотят обезопасить персональные данные волонтёров от возможной утечки. Какими способами можно гарантировать конфиденциальность?
Решение: Организаторы могут включить на сайте дополнительную меру защиты, такую как HTTPS (защищённое соединение через протокол Secure Socket Layer / Transport Layer Security). Помимо этого, собирать только минимальный набор данных, необходимых для участия, и ограничить доступ к собранной информации, оставив её доступной только ответственным лицам.

Примерный состав тестовых вопросов для проверки качества освоения дисциплины

Для контроля изученного материала обучаемому предлагается практическое тестовое задание не более чем на 30 минут, которое содержит 10 тестовых вопросов закрытого типа, за каждый правильный ответ начисляется 1 балл. Максимальное количество набранных баллов – 10.

1. **Программное средство для шифрования файлов и дисков, поддерживающее алгоритмы AES и Twofish, называется:**

A. WinRAR
B. VeraCrypt
C. Norton Antivirus
D. Malwarebytes

Правильный ответ: B. VeraCrypt

2. **Какой инструмент используют специалисты по информационной безопасности для анализа сетевого трафика?**

A. Ping
B. Speedtest
C. Netcat
D. Wireshark

Правильный ответ: D. Wireshark

3. **Назначение программы ClamAV заключается в следующем:**

A. Расшифровке зашифрованных файлов
B. Защите от спама и фишинга
C. Блокировке рекламы в браузере
D. Обнаружении и устранении вирусов и вредоносных программ

Правильный ответ: D. Обнаружении и устранении вирусов и вредоносных программ

4. **Алгоритм хеширования MD5 чаще всего применяют для:**

A. Шифрования сообщений электронной почты
B. Генерации случайных чисел
C. Контрольной суммы файлов
D. Передачи больших объемов данных

Правильный ответ: C. Контрольной суммы файлов

5. **К какому типу относится атака XSS (Cross-Site Scripting)?**

A. Атаки на доступность
B. Атаки на целостность
C. Атаки на конфиденциальность
D. Атаки на инфраструктуру

Правильный ответ: C. Атаки на конфиденциальность

6. **Бесплатный открытый инструмент для анализа и тестирования web-приложений на наличие уязвимостей называется:**

A. Acunetix
B. Burp Suite Professional
C. Nikto
D. QualysGuard

Правильный ответ: C. Nikto

7. **Какая технология позволяет анонимизировать IP-адрес пользователя в интернете?**

A. VPN
B. JavaScript
C. Cookie
D. SSL/TLS

Правильный ответ: A. VPN

8. **Безопасный способ аутентификации, использующий временные токены и дополнительные факторы подтверждения, называется:**

A. Однопроходная аутентификация
B. Двухфакторная аутентификация
C. Парольная аутентификация
D. Биометрическая аутентификация

Правильный ответ: B. Двухфакторная аутентификация

9. **Что такое SSL-сертификат?**

A. Сертификат подписи документа
B. Документ удостоверяющий личность пользователя
C. Цифровой сертификат, подтверждающий подлинность сервера и обеспечивающий безопасное соединение
D. Сертификат права собственности на доменное имя

Правильный ответ: C. Цифровой сертификат, подтверждающий подлинность сервера и обеспечивающий безопасное соединение

10. **Основной принцип предотвращения DoS/DDoS атак заключается в:**

A. Ограничении количества одновременных запросов
B. Увеличении пропускной способности канала
C. Переключении на резервные серверы
D. Повышении мощности оборудования

Правильный ответ: A. Ограничении количества одновременных запросов

11.Какой инструмент применяется для надежного шифрования данных на жестком диске или съемных накопителях?

A. TrueCrypt
B. BitLocker
C. Верракрипт (VeraCrypt)
D. FileVault

Правильный ответ: C. Верракрипт (VeraCrypt)

12.Что представляет собой метод TLS (Transport Layer Security)?

A.Метод шифрования файлов на компьютере
B.Технология защиты каналов передачи данных
C.Программа для мониторинга сети
D.Антивирусное решение

Правильный ответ: B. Технология защиты каналов передачи данных

13.Какой инструмент рекомендуется для детального анализа сетевого трафика?

A.WireShark
B.Metasploit
C.Nmap
D.John the Ripper
Правильный ответ: A. WireShark

14.Какой бесплатный инструмент рекомендован для поиска уязвимостей веб- приложений?

A,AppScan
B.Acunetix
C.OWASP ZAP
D.Fortify Scanning Tool
Правильный ответ: C. OWASP ZAP

15.Какая технология предотвращает утечку информации путем шифрования исходящего и входящего трафика?

A.VPN
B.HTTP
E. NS
D.SMTP
Правильный ответ: A. VPN

16.Какой метод шифрования рекомендуется для надежной защиты конфиденциальности данных?

A.RSA
B.SHA-256
C.Base64
D.XOR
Правильный ответ: A. RSA

17.Какой инструмент позволяет проверять состояние портов на компьютерах и устройствах в сети?

A.Snort
B.Nessus
C.Nmap
D.Kali Linux
Правильный ответ: C. Nmap

18.Какой инструмент помогает защититься от SQL-инъекций в веб-приложениях?

A.John the Ripper
B.Burp Suite Free Edition
C.Netsparker

D.Recon-ng

Правильный ответ: B. Burp Suite Free Edition

19.Какой инструмент полезен для комплексного анализа уязвимостей на стороне ОС и сетевых сервисов?

A.Dradis Framework

B.Vega Scanner

C.penVAS

D.RouterSploit

Правильный ответ: C. OpenVAS

11. Какой инструмент применяется для генерации сложных паролей и защиты от брутфорс-атак?

A. Python

B. LastPass Password Generator

C. John the Ripper

D. PuTTYgen

Правильный ответ: B. LastPass Password Generator

14.Какая мера необходима для защиты творческой работы от несанкционированного копирования и использования?

A. Установка водяного знака

B. Регистрация товарного знака

C. Патентование изобретения

D. Заключение договора аренды

Правильный ответ: A. Установка водяного знака

15.Как предотвратить распространение приватных инструкций по проведению занятий среди посторонних лиц?

A.Использование публичного облака для хранения файлов

B.Хранение файлов на флеш-накопителе

C.Передача файлов через социальные сети

D.Использование парольной защиты архива

Правильный ответ: D. Использование парольной защиты архива

16.Каким способом участники смогут безопасно передавать свои контактные данные организаторам мероприятия?

A.Через публичные чаты

B.Через регистрацию на официальном сайте организаторов с поддержкой протокола HTTPS

C.Через размещение объявлений в местных СМИ

D.Путём расклейки объявлений на улице

Правильный ответ: B. Через регистрацию на официальном сайте организаторов с поддержкой протокола HTTPS

17.Какой механизм защиты рекомендуется использовать при создании форм регистрации участников образовательных мероприятий?

A.Антибаннер

B.Электронный сертификат

C.CAPTCHA

D.Дополнительный Fдминистратор

Правильный ответ: C. CAPTCHA

18.Что поможет молодому специалисту защищать проекты от попадания в них вредных зависимостей и компонентов?

A.Покупка премиум-аккаунта GitHub

B.Тщательная проверка репутации поставщиков программных модулей с помощью OWASP Dependency Checker

C.Переход на закрытые исходники

D.Запрет на установку любых библиотек

Правильный ответ: B. Тщательная проверка репутации поставщиков программных модулей с помощью OWASP Dependency Checker

19. Как молодые организаторы мероприятия могут защитить базу данных волонтеров от неправомерного доступа?

A.Пользоваться обычными текстовыми файлами

B.Применять шифрование и хранение в специализированных защищённых сервисах, например, Google Таблицы с правами доступа

C. Оставлять распечатанные листы регистрации на столе

D. Позволить доступ к данным всем волонтёрам

Правильный ответ: B. Применять шифрование и хранение в специализированных защищённых сервисах, например, Google Таблицы с правами доступа

20. Что является важным элементом безопасности при проведении дистанционных лекций и семинаров?

A.Игнорирование настроек конфиденциальности вебинарных комнат

B.Открытый доступ ко всем материалам для публики

C.Наличие многоуровневой аутентификации участников мероприятия

D.Отсутствие проверки списков приглашённых

Правильный ответ. C. Наличие многоуровневой аутентификации участников мероприятия

21. Какой безопасный способ подойдёт для передачи конфиденциальных сведений о сотрудниках организации волонтёрскому штабу?

A. Публичный чат

B. Личная передача бумажных копий

C. Электронная почта с защитой PGP/GnuPG

D. Сообщение через СМС-сообщения

Правильный ответ: С. Электронная почта с защитой PGP/GnuPG

22. Какую роль играет применение шифрования при хранении важных организационно-методических документов в облаке?

A. Усложнение работы сотрудникам

B. Полная гарантия сохранности данных вне зависимости от обстоятельств

C. Возможность произвольного доступа к документам любым сотрудником

D. Защита данных от несанкционированного доступа при компрометации хранилища

Правильный ответ: D. Защита данных от несанкционированного доступа при компрометации хранилища

23. Какой инструмент пригодится молодым специалистам для защиты компьютеров от попыток проникновения хакеров?

A. Беспроводная клавиатура

B. Бесплатный антивирус, например, ClamAV

C. Модифицированная мышь

D. Веб-камера высокой чёткости

Правильный ответ: B. Бесплатный антивирус, например, ClamAV

6. КРИТЕРИИ ОЦЕНИВАНИЯ

Текущий контроль: активная работа на практических занятиях, выступления с докладами и сообщениями оценивается в баллах, от 2 до 5. Особой оценки заслуживает ведение диалога во время дискуссии (умение аргументировано высказать и отстаивать свою точку зрения).

Критерии оценки устных выступлений:

- оценка «отлично» выставляется, если студент дал правильный и развернутый ответ, привел факты и примеры;
- оценка «удовлетворительно» ставится, если студент не полный ответ;
- оценка «неудовлетворительно» ставится, если студент дал неправильный ответ.

Требования, предъявляемые к устному выступлению на практической работе:

• Логическое изложение индивидуального впечатления, соображения, видения по конкретному вопросу, претендующее на исчерпывающую полноту данного вопроса; оценивается стилистика автора, лаконичность изложения, интересные примеры, сравнения.

• Время – не более 5-7 минут.

• Выступление должно завершаться указанием на литературные источники или указанием адреса электронного ресурса.

Оценивается:

- содержательность выступления, раскрытие темы;
- знание теоретических источников по теме;
- аргументированное изложение собственного мнения по данной проблемам;

- использование иллюстративного материала (примеров, статистических данных и т.д);
- творческий подход к осмыслению предложенной темы;
- свободное владение материалом;
- уважение к оппоненту;
- вежливое поведение.

Текущий контроль (проверка) проводится регулярно на всех видах групповых занятий и имеет цель получать оперативную информацию о текущей успеваемости. Методами традиционного контроля являются устный и письменный опросы; контрольная беседа; проверка домашних заданий; ответы на вопросы, поставленные для самоконтроля и т.п. Оценочные средства для контроля сформированности компетенций содержатся в документе Оценочные материалы по дисциплине (ОМД).

Критерии оценки знаний на зачете/экзамене

Зачет выявляет знание базовых понятий, основных методов и направлений психологической науки, понимание основных подходов, фактов и закономерностей поведения человека в обществе.

Для оценки знаний, умений, навыков и формирования компетенции по дисциплине учитываются итоги выполнения практических заданий, устных выступлений и выполнение контрольных работ, а также ответ на вопрос, предложенный студенту на зачете.

К зачету допускаются студенты, выполнившие все виды учебных работ в течение семестра в установленные сроки. При условии пропусков занятий студенты должны выполнять их во внеаудиторное время.

Зачет выставляется, когда:

- студент показывает глубокое знание предмета обязательной и дополнительной литературы, аргументированно и логически стройно излагает материал, может применить знания для анализа конкретных ситуаций, профессиональных проблем;
- при твердых знаниях предмета, обязательной литературы, знакомстве с дополнительной литературой, аргументированном изложении материала, умении применить знания для анализа конкретных ситуаций, профессиональных проблем;
- когда студент в основном знает предмет, обязательную литературу, может практически применять свои знания.

Зачет не выставляется, когда:

- студент не усвоил основного содержания предмета и слабо знает рекомендованную литературу.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Перечень материально-технического обеспечения для реализации образовательного процесса по дисциплине:

1. Учебная аудитория для проведения занятий лекционного типа с мультимедийным оборудованием.
2. Учебная аудитория для проведения занятий семинарского (практического) типа, проведения групповых и индивидуальных консультаций, проведения текущего контроля и промежуточной аттестации.
3. Помещения для самостоятельной работы.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1Основная литература

- Суворова, Г. М. Информационная безопасность: учебное пособие / Г. М. Суворова. — 2-е изд. — Саратов: Вузовское образование, 2024. — 214 c. — ISBN 978-5-4487-1026-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/142805.html
- Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд. — Саратов: Профобразование, 2024. — 702 c. — ISBN 978-5-4488-0070-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/145912.html
- Информационная безопасность: учебное пособие / И. Б. Тесленко, Д. В. Виноградов, А. М. Губернаторов [и др.]; под редакцией И. Б. Тесленко. — Владимир: Издательство Владимирского государственного университета, 2023. — 212 c. — ISBN 978-5-9984-1783-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/143816.html

8.2. Дополнительная литература

1. Дронов, В. Ю. Информационная безопасность банковской деятельности: учебное пособие / В. Ю. Дронов, Г. А. Дронова. — Новосибирск: Новосибирский государственный технический университет, 2024. — 96 c. — ISBN 978-5-7782-5319-3. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/155872.html

2. Информационная безопасность и правовые основы защиты персональных данных: учебное пособие / А. В. Терехов, В. Н. Чернышов, А. В. Платенкин, А. В. Селезнев. — Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2023. — 80 c. — ISBN 978-5-8265-2648-4. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/141049.html

3. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. — Москва: Национальный исследовательский ядерный университет «МИФИ», 2023. — 224 c. — ISBN 978-5-7262-2949-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/132693.html

8.3 Программное обеспечение и Интернет-ресурсы

1. Электронная библиотека. Режим доступа https://www.iprbookshop.ru/