



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)
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
«Б1.О.19.06 ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 10.03.01 Информационная безопасность

Направленность(профиль) подготовки: Организация и технология защиты информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Москва, 2024

Разработчики:

Доцент кафедры Информационно-измерительных систем, к.э.н.
Трофимов С. В.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Минобрнауки от 17.11.2020 № 1427

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 способности решать задачи, связанные с организационными, методическими, управленческими и информационно-аналитическими технологиями для определения, профилактики, противодействия угрозам в информационной сфере и минимизации последствий их реализации, а также технологиями обеспечения информационной безопасности объектов различного назначения.

Задачи изучения дисциплины:

- получение устойчивого понимания и возможности практического использования знаний, умений и навыков по целям, задачам и принципам формирования хозяйствующих субъектов, а также основным направлениям обеспечения информационной безопасности в организациях, структурированных по разным принципам;
- изучение теоретических и практических методов выявления критических с точки зрения информационной уязвимости процессов функционирования хозяйствующих субъектов;
- формирование профессиональных компетенций в части ключевых управленческих задач и решений, направленных на обеспечение реализации организационных, методических и технических подходов к информационной безопасности;
- овладение основными терминами и определениями для анализа нормативно-правовой базы, угроз и рисков, классификации объектов исследования и разработки адекватных мер защиты информации.

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

Компетенции, индикаторы и результаты обучения

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

ОПК-10.1 Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики

Знать:

ОПК-10.1/Зн1 основные цели и задачи политики информационной безопасности как документа, регламентирующего стратегию и меры по защите информации в организации

Уметь:

ОПК-10.1/Ум1 анализировать требования организации и нормативных документов для формулировки целей и задач политики информационной безопасности

Владеть:

ОПК-10.1/Нв1 навыками разработки и документирования комплексной политики информационной безопасности с учетом современных стандартов и законодательства

ОПК-10.2 Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности

Знать:

ОПК-10.2/Зн1 процессы и методы организации выполнения мер информационной безопасности на объекте защиты

Уметь:

ОПК-10.2/Ум1 организовывать работу по внедрению и сопровождению мер информационной безопасности в соответствии с утвержденной политикой и нормативными требованиями

Владеть:

ОПК-10.2/Нв1 методиками проведения контроля, аудита и мониторинга информационной безопасности в операционных системах

ОПК-10.3 Осуществляет управление процессом обеспечения информационной безопасности

Знать:

ОПК-10.3/Зн1 основные компоненты и этапы процесса управления информационной безопасностью на объекте защиты

Уметь:

ОПК-10.3/Ум1 планировать и координировать выполнение комплекса мер по обеспечению информационной безопасности на объекте

Владеть:

ОПК-10.3/Нв1 навыками системного подхода к управлению процессами обеспечения информационной безопасности

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.19.06 «Основы управления информационной безопасностью» относится к обязательной части образовательной программы и изучается в семестре(ах): 7.

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)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
7 семестр	108	3	34	34	40	Зачет
Всего	108	3	34	34	40	

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Лекционные занятия	Практические занятия	Самостоятельная работа	Учебные результаты, соответствующие компетенциям

	Всего	Лекции	Практи	Самост	Планир обучен результ програ
Раздел 1. Понятие «Организационной защиты информации»	44	12	20	12	ОПК-10.2 ОПК-10.3
Тема 1.1. Сущность управления информационной безопасностью	0,5	0,5			
Тема 1.2. Принципы формирования (типы) организационных структур и регламентации их деятельности	8,5	0,5	8		
Тема 1.3. Линейно-функциональная организационная структура, принципы построения и функционирования	3	1		2	
Тема 1.4. Дивизиональная организационная структура, принципы построения и функционирования	1	1			
Тема 1.5. Особенности подчинения региональных структур службы безопасности в дивизиональных организациях	1	1			
Тема 1.6. Матричная организационная структура, принципы построения и функционирования	1	1			
Тема 1.7. Процессная организационная структура, принципы построения и функционирования	1	1			
Тема 1.8. Общая структура подразделений службы безопасности, задачи, решаемые каждым из них	9	1	8		
Тема 1.9. Внутренняя регламентация, как основа работы службы безопасности	1	1			
Тема 1.10. Внешняя регламентация деятельности по защите информации (федеральное законодательство)	1	1			
Тема 1.11. Стандартизация процессного описания	7	1	4	2	
Тема 1.12. Стандарт описания IDEF, его значение в области международной и российской практики управленческой стандартизации	1	1			

Тема 1.13. Отчетно-учетные методы ограничения доступа к информации (каскадное моделирование отчетно-учетной системы организации)	1	1			
Тема 1.14. Создание концепции защиты предприятия	4			4	
Тема 1.15. Создание службы информационной безопасности, организационная структура и основные функции	4			4	
Раздел 2. Организационные источники и каналы утечки. Силы, средства и условия организационной защиты информации	22	8		14	ОПК-10.1 ОПК-10.2 ОПК-10.3
Тема 2.1. Каналы утечки информации	2,5	0,5		2	
Тема 2.2. Причины утечки информации	0,5	0,5			
Тема 2.3. Контроль исполнения документов	2	2			
Тема 2.4. Технологические системы защиты и обработки конфиденциальных документов	2	2			
Тема 2.5. Общая логика процесса защищенного документооборота	2	2			
Тема 2.6. Особенность построения корпоративной безопасности в условиях экономического кризиса	5	1		4	
Тема 2.7. Информация, представляющая интерес при сборе и анализе сведений в разрезе современных способов атак на пользователей различных информационных ресурсов и систем	4			4	
Тема 2.8. Методы и технологии OSINT	4			4	
Раздел 3. Порядок подбора и текущая работа с персоналом. Организация допуска к различного рода информации и контроль ее сохранности	28	10	8	10	ОПК-10.1 ОПК-10.2 ОПК-10.3
Тема 3.1. Задачи построения системы безопасности, основные угрозы безопасности, принципы и средства организации обеспечения безопасности	6	2	4		

Тема 3.2. Информация, представляющая интерес при сборе и анализе сведений	4,5	0,5	4		
Тема 3.3. Классификация угроз безопасности информации	0,5	0,5			
Тема 3.4. Угрозы, не связанные с деятельностью человека	0,5	0,5			
Тема 3.5. Угрозы, связанные с деятельностью человека	0,5	0,5			
Тема 3.6. Порядок подбора и увольнения персонала, роль службы безопасности в этом процессе	2	2			
Тема 3.7. Управление в чрезвычайных ситуациях	2	2			
Тема 3.8. Утечка акустической информации из-за применения подслушивающих устройств	0,5	0,5			
Тема 3.9. Пути утечки информации в вычислительных системах	0,5	0,5			
Тема 3.10. Утечка информации за счет ПЭМИН	0,5	0,5			
Тема 3.11. Утечка информации при использовании средств связи и различных проводных коммуникаций	0,5	0,5			
Тема 3.12. Работа с персоналом в части организации допуска к сведениям ограниченного доступа	10			10	
Раздел 4. Аналитическая работа и контроль функционирования системы организационной защиты информации, как основа управления системой организационной защиты информации	14	4	6	4	ОПК-10.1 ОПК-10.2 ОПК-10.3
Тема 4.1. Корпоративная разведка и промышленный шпионаж, сущность и отличия	8,5	0,5	6	2	
Тема 4.2. Закрытые открытые источники в конкурентной разведке	2,5	0,5		2	
Тема 4.3. Рекрутинг, как средство конкурентной разведки	1	1			
Тема 4.4. Тайное физическое проникновение	1	1			
Тема 4.5. "Дилерские" подходы	1	1			
Итого	108	34	34	40	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Понятие «Организационной защиты информации»

Тема 1.1. Сущность управления информационной безопасностью

Раскрывается понятие ИБ как процесса, определяются цели управления (обеспечение конфиденциальности, целостности и доступности информации), объекты управления и роль руководителя в этом процессе.

Тема 1.2. Принципы формирования (типы) организационных структур и регламентации их деятельности

Обзор основных типов структур управления (иерархические, адаптивные), принципы их построения (единоначалие, специализация), а также важность создания регламентов (положений, инструкций) для упорядочивания работы.

Тема 1.3. Линейно-функциональная организационная структура, принципы построения и функционирования

Изучение классической структуры, где линейные руководители принимают решения, а функциональные подразделения (кадры, бухгалтерия, безопасность) обеспечивают экспертизу. Рассматриваются достоинства (стабильность) и недостатки (медленная реакция на изменения).

Тема 1.4. Дивизиональная организационная структура, принципы построения и функционирования

Анализ структуры, построенной по продуктовому, региональному или потребительскому признаку. Показывается, как дивизионы обладают самостоятельностью, что требует децентрализации функций, включая безопасность.

Тема 1.5. Особенности подчинения региональных структур службы безопасности в дивизиональных организациях

Рассматриваются проблемы двойного подчинения сотрудников СБ на местах (руководителю дивизиона и центральному аппарату СБ), варианты матричного подчинения и конфликты интересов.

Тема 1.6. Матричная организационная структура, принципы построения и функционирования

Описание гибкой структуры, где сотрудники подчиняются одновременно функциональному руководителю и руководителю проекта. Анализ сложностей управления, в том числе для службы безопасности, контролирующей персонал в проектах.

Тема 1.7. Процессная организационная структура, принципы построения и функционирования

Переход от иерархии к управлению бизнес-процессами. Рассматривается, как служба безопасности встраивается в сквозные процессы компании (например, «Разработка продукта» или «Работа с заказчиком»), а не существует как изолированный отдел.

Тема 1.8. Общая структура подразделений службы безопасности, задачи, решаемые каждым из них

Детализация типовой структуры службы безопасности: режимно-секретное подразделение, отдел защиты информации, отдел физической охраны, отдел экономической безопасности, их функции и зоны ответственности.

Тема 1.9. Внутренняя регламентация, как основа работы службы безопасности

Изучение комплекта внутренних документов (политики ИБ, инструкции, приказы, положения), которые формализуют правила работы с конфиденциальной информацией и ответственность сотрудников.

Тема 1.10. Внешняя регламентация деятельности по защите информации (федеральное законодательство)

Обзор российских законов (ФЗ «О безопасности», «О коммерческой тайне», «О персональных данных», «Об информации...»), устанавливающих правовые основы и требования к защите информации.

Тема 1.11. Стандартизация процессного описания

Введение в понятие стандартов, регламентирующих, как именно нужно описывать деятельность компании (ISO, ГОСТы), чтобы обеспечить прозрачность и возможность аудита процессов.

Тема 1.12. Стандарт описания IDEF, его значение в области международной и российской практики управленческой стандартизации

Рассмотрение семейства методологий (IDEF0) для моделирования бизнес-процессов. Показывается, как с помощью IDEF можно наглядно описать, где в процессах возникают риски ИБ.

Тема 1.13. Отчетно-учетные методы ограничения доступа к информации (каскадное моделирование отчетно-учетной системы организации)

Изучение методов учета (журналы, акты, электронные системы), позволяющих отследить движение документов и доступ к данным, а также каскадный принцип распределения прав доступа.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 1.14. Создание концепции защиты предприятия

Этапы формирования стратегического документа, определяющего, что именно нужно защищать, от кого и какими методами, с учетом специфики бизнеса.

Тема 1.15. Создание службы информационной безопасности, организационная структура и основные функции

Практические шаги по формированию СИБ «с нуля»: определение штатной численности, выбор места в оргструктуре, набор функций и взаимодействие с другими подразделениями.

Раздел 2. Организационные источники и каналы утечки. Силы, средства и условия организационной защиты информации

Тема 2.1. Каналы утечки информации

Классификация физических и технических путей несанкционированного получения данных (через людей, документы, технику, излучения).

Тема 2.2. Причины утечки информации

Анализ человеческого фактора (халатность, мотивация, злой умысел), несовершенства организационных процедур и технических средств.

Тема 2.3. Контроль исполнения документов

Рассмотрение системы отслеживания движения распорядительных и конфиденциальных документов как способ предотвращения потерь и утечек.

Тема 2.4. Технологические системы защиты и обработки конфиденциальных документов

Обзор специализированного ПО и оборудования (DLP-системы, СКЗД, системы электронного документооборота с грифом секретности) для безопасной работы с документами.

Тема 2.5. Общая логика процесса защищенного документооборота

Описание жизненного цикла документа (создание — учет — хранение — использование — уничтожение) и контрольных точек на каждом этапе.

Тема 2.6. Особенность построения корпоративной безопасности в условиях экономического кризиса

Антикризисные меры: усиление контроля за лояльностью персонала (риск увольнений), защита от недружественных поглощений, оптимизация расходов на безопасность без потери эффективности.

Текущий контроль	
Вид (форма) контроля	
Тестирование	

Тема 2.7. Информация, представляющая интерес при сборе и анализе сведений в разрезе современных способов атак на пользователей различных информационных ресурсов и систем

Что ищут злоумышленники (учетные данные, служебная переписка, коммерческие тайны) с помощью фишинга, социальной инженерии и других атак.

Тема 2.8. Методы и технологии OSINT

Изучение технологий сбора и анализа информации из открытых источников (соцсети, СМИ, базы данных) как инструмента для проверки контрагентов и поиска уязвимостей.

Раздел 3. Порядок подбора и текущая работа с персоналом. Организация допуска к различного рода информации и контроль ее сохранности

Тема 3.1. Задачи построения системы безопасности, основные угрозы безопасности, принципы и средства организации обеспечения безопасности

Обобщающее введение в системный подход к защите от всего спектра угроз.

Тема 3.2. Информация, представляющая интерес при сборе и анализе сведений

Детализация, какие именно данные о компании (финансы, клиенты, разработки) являются целевыми для конкурентов и мошенников.

Тема 3.3. Классификация угроз безопасности информации

Разделение угроз по природе возникновения (природные, техногенные, антропогенные), по умыслу (случайные, преднамеренные) и по источнику.

Тема 3.4. Угрозы, не связанные с деятельностью человека

Рассмотрение форс-мажоров: пожары, наводнения, аварии электросетей, ведущие к потере данных или нарушению работы.

Тема 3.5. Угрозы, связанные с деятельностью человека

Анализ инсайдеров (обиженные сотрудники, шпионы), ошибок персонала, хакерских атак.

Тема 3.6. Порядок подбора и увольнения персонала, роль службы безопасности в этом процессе

Процедуры проверки кандидатов (служба безопасности «пробивает» соискателя), сопровождение допуска к секретам и процедура «закрытия доступа» при увольнении.

Тема 3.7. Управление в чрезвычайных ситуациях

Действия служб при инцидентах (пожар, теракт, обнаружение взломанной системы), планы эвакуации и сохранности носителей.

Тема 3.8. Утечка акустической информации из-за применения подслушивающих устройств

Каналы перехвата речи, методы защиты (виброакустика, генераторы шума) и поиск закладных устройств.

Тема 3.9. Пути утечки информации в вычислительных системах

Сетевые атаки, вредоносное ПО, съемные носители, несанкционированный копирование.

Тема 3.10. Утечка информации за счет ПЭМИН

Физический процесс возникновения побочных электромагнитных излучений и наводок от мониторов, кабелей, принтеров, позволяющий снимать информацию дистанционно.

Тема 3.11. Утечка информации при использовании средств связи и различных проводных коммуникаций

Перехват факсов, телефонных переговоров, подключение к витой паре или оптоволокну.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 3.12. Работа с персоналом в части организации допуска к сведениям ограниченного доступа

Инструктажи, подписки о неразглашении, обучение правилам работы 机密 (конфиденциальными) данными.

Раздел 4. Аналитическая работа и контроль функционирования системы организационной защиты информации, как основа управления системой организационной защиты информации

Тема 4.1. Корпоративная разведка и промышленный шпионаж, сущность и отличия

Разграничение понятий: легальный сбор и анализ данных о рынке и конкурентах (КР) и незаконное добывание секретов (шпионаж).

Тема 4.2. Закрытые открытые источники в конкурентной разведке

Понятие о том, что ценная информация часто находится в открытом доступе, но требует аналитической обработки.

Тема 4.3. Рекрутинг, как средство конкурентной разведки

Методы получения информации через переманивание сотрудников конкурента или внедрение «своего» человека под видом соискателя.

Тема 4.4. Тайное физическое проникновение

Методы нелегального доступа на объекты (кражи, копирование документов, установка «жучков») и методы противодействия им.

Тема 4.5. "Дилерские" подходы

Изучение методов получения информации через перекупщиков, дилеров или перехват управления дилерскими сетями для доступа к клиентской базе или технологиям.

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, 7 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 1. Понятие «Организационной защиты информации»

Контролируемые ИДК: ОПК-10.2 ОПК-10.3

Тема 1.13. Отчетно-учетные методы ограничения доступа к информации (каскадное моделирование отчетно-учетной системы организации)

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие три принципа составляют CIA-триаду?
 1. Аутентичность, Достоверность, Надежность
 2. Конфиденциальность, Целостность, Доступность
 3. Шифрование, Аутентификация, Авторизация
 4. Угрозы, Уязвимости, Риски
 5. Защита, Контроль, Мониторинг
2. Какой стандарт является международным для систем управления информационной безопасностью?
 1. ISO/IEC 27001
 2. ГОСТ Р 57580
 3. NIST SP 800-53
 4. PCI DSS
 5. GDPR
3. Какой закон РФ регулирует защиту персональных данных?
 1. ФЗ-152
 2. ФЗ-149

3. ФЗ-161
4. ФЗ-187
5. ФЗ-63

4. Что такое уязвимость в контексте информационной безопасности?

1. Действие злоумышленника
2. Слабое место в системе
3. Вид вредоносного ПО
4. Метод шифрования
5. Политика безопасности

5. Какой принцип предполагает минимально необходимые права доступа?

1. Разделение обязанностей
2. Минимальные привилегии
3. Экономическая целесообразность
4. Полная прозрачность
5. Коллективная ответственность

6. Какой этап управления рисками включает идентификацию активов?

1. Оценка угроз
2. Расчет рисков
3. Принятие риска
4. Мониторинг
5. Аудит

7. Какие методы используются для снижения рисков? (Выберите два)

1. Внедрение межсетевых экранов
2. Страхование киберрисков
3. Игнорирование угроз
4. Удаление резервных копий
5. Отключение антивирусов

8. Какой инструмент анализа рисков разработан NIST?

1. OCTAVE
2. NIST SP 800-30
3. FAIR
4. ISO 27005
5. COBIT

9. Какой метод оценки рисков основан на экспертных оценках?

1. Качественный
2. Количественный
3. Статистический
4. Вероятностный
5. Аналитический

10. Какой метод снижения рисков предполагает передачу ответственности страховой компании?

1. Избежание риска
2. Страхование
3. Принятие риска
4. Минимизация
5. Игнорирование

Раздел 2. Организационные источники и каналы утечки. Силы, средства и условия организационной защиты информации

Контролируемые ИДК: ОПК-10.1 ОПК-10.2 ОПК-10.3

Тема 2.6. Особенность построения корпоративной безопасности в условиях экономического кризиса

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой этап построения СУИБ включает разработку политик?

1. Планирование
2. Внедрение
3. Эксплуатация
4. Аудит
5. Улучшение

2. Какие меры относятся к техническим контрмерам? (Выберите два)

1. Шифрование данных
2. Межсетевые экраны
3. Обучение сотрудников
4. Разработка регламентов
5. Страхование

3. Какой документ регламентирует правила использования паролей?

1. Политика информационной безопасности
2. План реагирования
3. Регламент резервного копирования
4. Договор с поставщиком
5. Инструкция пользователя

4. Какой этап жизненного цикла СУИБ включает мониторинг?

1. Планирование
2. Эксплуатация
3. Внедрение
4. Аудит
5. Улучшение

5. Что такое SOC?

1. Центр мониторинга безопасности
2. Система обнаружения вторжений
3. Программа шифрования
4. Стандарт безопасности
5. Метод оценки рисков

6. Какой метод шифрования использует один ключ?

1. Симметричное
2. Асимметричное
3. Хеширование
4. Электронная подпись
5. Квантовое

7. Какие функции обеспечивает электронная подпись? (Выберите два)

1. Аутентификацию
2. Целостность
3. Шифрование
4. Защиту от DDoS
5. Блокировку вирусов

8. Какой инструмент защищает сеть от несанкционированного доступа?

1. Межсетевой экран
2. Антивирус
3. VPN
4. SIEM
5. IDS

9. Что такое VPN?

1. Защищенное сетевое соединение

2. Система обнаружения атак
 3. Метод шифрования
 4. Средство резервного копирования
 5. Инструмент аутентификации
10. Какой тип вредоносного ПО требует выкуп?

1. Ransomware
2. Троян
3. Червь
4. Spyware
5. Adware

Раздел 3. Порядок подбора и текущая работа с персоналом. Организация допуска к различного рода информации и контроль ее сохранности

Контролируемые ИДК: ОПК-10.1 ОПК-10.2 ОПК-10.3

Тема 3.11. Утечка информации при использовании средств связи и различных проводных коммуникаций

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой этап инцидента включает сбор доказательств?
 1. Подготовка
 2. Расследование
 3. Сдерживание
 4. Ликвидация
 5. Восстановление
2. Какие системы используются для мониторинга безопасности? (Выберите два)
 1. SIEM
 2. Антивирус
 3. IDS/IPS
 4. Фаервол
 5. VPN
3. Какой документ определяет порядок действий при инциденте?
 1. Политика паролей
 2. План реагирования
 3. Регламент копирования
 4. Договор с поставщиком
 5. Инструкция пользователя
4. Какой этап инцидента включает восстановление системы?
 1. Обнаружение
 2. Анализ
 3. Восстановление
 4. Документирование
 5. Улучшение
5. Какие преимущества дает SOC?
 1. Круглосуточный мониторинг
 2. Автошифрование
 3. Быстрое реагирование
 4. Упрощение паролей
 5. Отказ от антивирусов
6. Какой стандарт используется для сертификации СУИБ?
 1. ISO/IEC 27001
 2. PCI DSS

3. GDPR
4. NIST CSF
5. COBIT

7. Какие виды аудита существуют? (Выберите два)

1. Внутренний
2. Внешний
3. Автоматический
4. Случайный
5. Поверхностный

8. Какой стандарт регулирует безопасность платежных данных?

1. ISO 27001
2. PCI DSS
3. HIPAA
4. FSTEC
5. SOX

9. Какой этап аудита включает рекомендации?

1. Планирование
2. Сбор данных
3. Отчетность
4. Проверка
5. Сертификация

10. Что такое корректирующие действия?

1. Устранение несоответствий
2. Планирование аудита
3. Назначение ответственных
4. Разработка политик
5. Проведение тренингов

Раздел 4. Аналитическая работа и контроль функционирования системы организационной защиты информации, как основа управления системой организационной защиты информации

Контролируемые ИДК: ОПК-10.1 ОПК-10.2 ОПК-10.3

Тема 4.5. "Дилерские" подходы

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие риски связаны с IoT?

1. Недостаточная защита данных
2. Увеличение скорости интернета
3. Создание ботнетов
4. Улучшение связи
5. Снижение стоимости оборудования

2. Как ИИ применяется в информационной безопасности?

1. Анализ аномалий трафика
2. Уменьшение паролей
3. Отказ от антивирусов
4. Упрощение аудита
5. Снижение стоимости оборудования

3. Какое влияние оказывает GDPR?

1. Защита персональных данных ЕС
2. Свободный обмен данными
3. Отмена паролей
4. Упрощение аудита

5. Снижение требований к шифрованию

4. Что такое "угрозы нулевого дня"?

1. Уязвимости без патчей
2. Атаки в полночь
3. Угрозы квантовых компьютеров
4. Риски устаревшего оборудования
5. Проблемы обновлений

5. Какие технологии относятся к перспективным?

1. Квантовое шифрование
2. Отказ от паролей
3. Биометрическая аутентификация
4. Упрощенное логирование
5. Открытый доступ

6. Что такое "красная команда"?

1. Разработчики антивирусов
2. Специалисты по тестированию защиты
3. Техподдержка
4. Отдел продаж
5. Аналитики логов

7. Какой метод эффективен против социальной инженерии?

1. Увеличение длины паролей
2. Обучение сотрудников
3. Дополнительные серверы
4. Отключение интернета
5. Шифрование всех данных

8. Что проверяет тест на проникновение?

1. Уязвимости защиты
2. Скорость интернета
3. Качество бэкапов
4. Удобство интерфейса
5. Стоимость оборудования

9. Какой показатель измеряет эффективность защиты?

1. Количество сотрудников
2. Время реагирования
3. Стоимость оборудования
4. Количество паролей
5. Частота обновлений

10. Какой принцип реализует многофакторная аутентификация?

1. Открытый доступ
2. Усиленная проверка
3. Анонимность
4. Минимальные требования
5. Автоход

8. Оценочные материалы промежуточной аттестации

7 семестр, Зачет

Контролируемые ИДК: ОПК-10.1 ОПК-10.2 ОПК-10.3

Вопросы/Задания:

1. Принципы формирования (типы) организационных структур и регламентации их деятельности.

2. Линейно-функциональная организационная структура, принципы построения и функционирования. Место службы безопасности в ЛФОС.
3. Дивизиональная организационная структура, принципы построения и функционирования. Место службы безопасности в дивизиональной оргструктуре.
4. Особенности подчинения региональных структур службы безопасности в дивизиональных организациях. Модель матричного взаимодействия структурных подразделений.
5. Матричная организационная структура, принципы построения и функционирования. Понятия «слабой» и «сильной» матрицы. Подчинение по отдельным вопросам работы. Проектная матрица.
6. Процессная организационная структура, принципы построения и функционирования. Модель работы СБ в процессных структурах.
7. Функции, задачи и структура службы безопасности предприятия
8. Создание концепции безопасности на примере финансовой организации (банка)
9. Проектирование структуры службы безопасности
10. Функции, задачи и особенности деятельности подразделений службы безопасности
11. Создание службы информационной безопасности, организационная структура и основные функции
12. Служба безопасности объекта. Типовая структура службы безопасности.
13. Организация пропускного и внутри объектового режимов.
14. Общие принципы внутренней регламентации
15. Объекты и субъекты обеспечения безопасности
16. Внешняя регламентация деятельности по ЗИ (федеральное законодательство)
17. Стандартизация процессного описания
18. Стандарт описания IDEF, его значение в области международной и российской практики управленческой стандартизации
19. Отчетно-учетные методы ограничения доступа к информации (каскадное моделирование отчетно-учетной системы организации)
20. Каналы утечки информации
21. Причины утечки информации

22. Контроль исполнения документов
23. Технологические процедуры контроля исполнения документов
24. Технологические системы защиты и обработки конфиденциальных документов
25. Общая логика процесса защищенного документооборота
26. Задачи построения системы корпоративной безопасности
27. Основные виды угроз интересам компании
28. Организация и функционирование системы безопасности компании
29. Средства обеспечения безопасности
30. Подсистемы системы безопасности компании
31. Способы и особенности функционирования Служб безопасности организаций
32. Проверка работы Службы безопасности
33. Подготовка к созданию системы безопасности компании
34. Особенности построения корпоративной безопасности в условиях экономического кризиса
35. Информация, представляющая интерес при сборе и анализе сведений
36. Классификация угроз безопасности информации
37. Угрозы, не связанные с деятельностью человека
38. Угрозы, связанные с деятельностью человека
39. Порядок подбора и увольнения персонала, роль Службы безопасности в этом процессе
40. Управление в чрезвычайных ситуациях
41. Утечка акустической информации из-за применения подслушивающих устройств
42. Пути утечки информации в вычислительных системах
43. Утечка информации за счет побочных электромагнитных излучения и наводки (ПЭМИН)
44. Утечка информации при использовании средств связи и различных проводных коммуникаций

45. Корпоративная (конкурентная) разведка и промышленный шпионаж, сущность и отличия
46. Закрытые и открытые источники в конкурентной разведке
47. Рекрутинг, как средство конкурентной разведки
48. Тайное физическое проникновение
49. "Дилерские" подходы

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Формализация подхода к определению актуальности угроз информационной безопасности: монография: монография / О. М. Голембиовская, М. Ю. Рытов, М. М. Голембиовский [и др.] - Формализация подхода к определению актуальности угроз информационной безопасности - Саратов: Вузовское образование, 2022. - 147 с. - 978-5-4487-0840-4. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/121143.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
2. Газизов А. Р. Управление информационной безопасностью: учебное пособие: учебное пособие / А. Р. Газизов, С. Б. Петренкова, Д. В. Фатхи. - Управление информационной безопасностью - Ростов-на-Дону: Донской государственный технический университет, 2019. - 115 с. - 978-5-7890-1775-3. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/117771.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
3. Шилов А. К. Управление информационной безопасностью: учебное пособие: учебное пособие / А. К. Шилов. - Управление информационной безопасностью - Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018. - 120 с. - 978-5-9275-2742-7. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/87643.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации: учебное пособие: учебное пособие / О. М. Голембиовская, М. Ю. Рытов, К. Е. Шинаков [и др.] - Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации - Саратов: Вузовское образование, 2024. - 265 с. - 978-5-4487-0942-5. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/134999.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
2. Анисимов А. А. Менеджмент в сфере информационной безопасности: учебное пособие: учебное пособие / А. А. Анисимов. - Менеджмент в сфере информационной безопасности - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 210 с. - 978-5-4497-2408-3. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/133946.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.elibrary.ru/> - НЭБ eLIBRARY
2. <https://znanium.ru/> - Электронно-библиотечная система "Znanium"
3. <https://rusneb.ru/> - Национальная электронная библиотека (НЭБ)
4. <https://www.iprbookshop.ru/> - IPR BOOKS
5. <https://e.lanbook.com/> - Электронная библиотечная система "Лань"

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 Office;

Перечень информационно-справочных систем

(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс

Автоматизированное рабочее место (АРМ) - 15 шт.

Доска настенная одноэлементная - 2 шт.

Проектор - 1 шт.

Смешанный тип

Автоматизированное рабочее место (АРМ) - 1 шт.

Доска настенная одноэлементная - 2 шт.

Интерактивная панель - 1 шт.

Проектор - 1 шт.

Учебная аудитория

Автоматизированное рабочее место (АРМ) - 6 шт.

Доска настенная одноэлементная - 1 шт.

Проектор - 1 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.

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.