МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ
СОВРЕМЕННЫЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАТИКИ

«Согласовано»
Начальник учебной части
_____Ерке Е.Э.
«25» 08 2024 г.

«Утверждаю»
I-проректор СМУ
_____Максат Макамбай
«_____»_____20___г.

РАБОЧАЯ ПРОГРАММА
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

для специальности (направления специальности): **710300 – Прикладная информатика**
Форма обучения: очная/заочная
Виды учебной деятельности:

Программа	Всего часов				СРС	СРСП	Форма отчетности
	всего	аудиторных	лекция	Прак.раб			
4-курс, 8 семестр (О/О)	5 кр 150 час	75	30	45	45 ч	30 ч	экзамен
4-курс, 8 семестр (З/О)	5 кр 150 час	40	20	20	70 ч	40 ч	экзамен

«Согласовано»
Профилирующей кафедрой
_____зав.каф.
от «_____»_____20___г.

«Рассмотрено»
на заседании кафедры
_____
от «_____»_____20__ г.

Рабочая программа дисциплины разработана в соответствии с ГОС (1578/1 от 21 сентября 2021 г), ОПОП направления 510200 - Прикладная математика и информатика, 710300 – Прикладная информатикаи Положения о разработке УМК в СМУ.

Разработчик: Кошбаев А.А.

Жалал-Абад
2024 г.

Содержание

1.1 Реквизиты дисциплины

Дисциплина : «Информационная безопасность»

Курс: 4

Направление: 710300 – Прикладная информатика

Количество кредит часов: 5мкр (150 ч)

Форма обучения: очная/заочная

1.2. Объем дисциплины и виды учебной работы

Вид учебной работы	Семестр 8 Всего часов 150 ч (О/О)	Семестр 8 Всего часов150 ч (З/О)
Аудиторные занятия (всего)	**75**	**40**
В том числе:		
Лекции (Л)	30	20
Практические занятия (ПЗ)	45	20
Семинары (С)		
Лабораторные практикумы (ЛП)		
Клинические практические занятия (КПЗ)		
Самостоятельная работа (всего)	**75**	**110**
СРСП	30	40
СРС	45	70
Форма контроля	экзамен	экзамен
Общая трудоемкость (час.)	**150 ч**	**150 ч**

2. Место дисциплины в структуре ООП

Учебная дисциплина «Информационная безопасность» является специальной дисциплиной, формирующей профессиональные знания, необходимые для будущей профессиональной деятельности.

Дисциплина относится к базовой части профессионального цикла.

3. Пререквизиты и постреквизиты курса

Пререквизиты (входные знания и дисциплины)

Перед изучением дисциплины *«Информационная безопасность»* студент должен освоить следующие дисциплины и области знаний:

1. **Информатика и основы программирования**

— базовые навыки работы с компьютером, понимание архитектуры

вычислительных систем, знание принципов хранения и обработки данных.

2. **Операционные системы**
   — знание структуры ОС, прав доступа, управления процессами и файловыми системами.
3. **Компьютерные сети и телекоммуникации**
   — основы сетевых архитектур, протоколов, адресации и передачи данных.
4. **Математическая логика и основы криптографии** *(желательно)*
   — понимание принципов шифрования, хеширования, аутентификации.
5. **Правоведение или правовые основы ИКТ**
   — базовые знания законодательства в области защиты информации и персональных данных.

Постреквизиты (дисциплины, для которых «Информационная безопасность» является основой)

Освоение курса *«Информационная безопасность»* необходимо для успешного изучения и прохождения следующих дисциплин и практик:

1. **Криптографические методы защиты информации**
   — углублённое изучение алгоритмов шифрования, электронных подписей, протоколов безопасности.
2. **Администрирование и защита информационных систем**
   — настройка политик безопасности, мониторинг, защита сетей и систем.
3. **Безопасность сетей и веб-приложений**
   — анализ уязвимостей, настройка firewall, IDS/IPS, безопасность передачи данных.
4. **Оценка рисков и управление ИБ**
   — методики анализа угроз, разработка политик безопасности, аудит ИБ.
5. **Информационное право и этика**
   — юридические аспекты безопасности, защита персональных данных, нормативные документы.
6. **Практика и ВКР (выпускная квалификационная работа)**
   — применение знаний по ИБ в реальных проектах, обоснование технических и организационных мер защиты.

4. Необходимость изучения курса

В условиях цифровизации всех сфер жизни и деятельности общества, безопасность информации становится одним из ключевых факторов устойчивого функционирования государственных органов, бизнеса и образовательных учреждений. Нарушения конфиденциальности, целостности и доступности информации приводят к серьёзным экономическим, правовым и репутационным последствиям.

Изучение дисциплины **«Информационная безопасность»** необходимо для:

- формирования у студентов системного понимания угроз и рисков в информационной среде;
- освоения базовых принципов защиты информации в компьютерных системах и сетях;
- изучения механизмов и технологий обеспечения безопасности данных;
- приобретения практических навыков анализа уязвимостей и реагирования на инциденты;
- понимания нормативно-правовой базы и стандартов в области ИБ;
- подготовки к профессиональной деятельности в области ИТ и ИБ.

Курс является фундаментальной составляющей подготовки современного ИТ-специалиста и закладывает основу для дальнейшего изучения дисциплин, связанных с криптографией, администрированием, аудитом ИБ и правовыми аспектами защиты информации.

5. Цели и задачи курса

Цель курса

Сформировать у студентов системное представление об основах информационной безопасности, изучить принципы, методы и средства защиты информации от несанкционированного доступа, разрушения, модификации и других угроз в информационных системах, а также подготовить к практическому применению этих знаний в профессиональной деятельности.

Задачи курса

1. **Познакомить с ключевыми понятиями и принципами информационной безопасности:**
   — конфиденциальность, целостность, доступность, подотчётность и отказоустойчивость.

2. **Изучить основные типы угроз и уязвимостей информации:**
   — внешние и внутренние угрозы, человеческий фактор, программные и технические уязвимости.
3. **Овладеть методами и средствами защиты информации:**
   — идентификация и аутентификация, криптографическая защита, антивирусные средства, межсетевые экраны, системы обнаружения вторжений.
4. **Изучить архитектуру систем безопасности в ИС и компьютерных сетях:**
   — модели управления доступом, разграничение прав, политики безопасности.
5. **Развить навыки оценки рисков и анализа инцидентов безопасности:**
   — выявление угроз, классификация инцидентов, план реагирования.
6. **Ознакомить с нормативно-правовыми и организационными аспектами ИБ:**
   — законы, стандарты, регламенты (например, ФЗ-152, ISO/IEC 27001, ГОСТы и др.).
7. **Подготовить студентов к практической реализации механизмов защиты информации:**
   — настройка ОС, защита сетей, использование программных средств ИБ.

6. Компетенции обучающегося, формируемые в результате освоения дисциплины

Код компетенции	Компетенция	Знания	Умения	Навыки
ПК-1	Способен использовать нормативно-правовые документы, международные и отечественные стандарты в области ИС и технологий	— Основы законодательства в области ИБ (в т.ч. ФЗ-152, ФЗ-149, GDPR и др.)— Стандарты безопасности: ISO/IEC 27001, ГОСТ Р 57580, NIST	— Анализировать требования нормативных документов к системам ИБ— Применять стандарты при разработке и оценке систем защиты информации	— Работа с регламентами, политиками безопасности— Оформление документации по ИБ— Подготовка отчётов и обоснований

Код компетенции	Компетенция	Знания	Умения	Навыки
ПК-12	Способен выбирать состав аппаратно-программного комплекса технических средств обработки информации и коммуникации	— Основы построения ИС, сетевых и вычислительных архитектур— Компоненты систем ИБ: межсетевые экраны, антивирусы, СКЗИ и др.	— Оценивать технические характеристики средств защиты информации— Подбирать компоненты с учётом рисков и требований ИБ	— Конфигурирование и сравнение средств защиты— Создание схем ИС с учетом ИБ— Сбор ТТХ и обоснование выбора
ПК-13	Способен принимать участие в реализации профессиональных коммуникаций в рамках проектных групп, обучать пользователей ИС	— Основы делового общения и командной работы— Принципы взаимодействия в ИТ-проектной среде— Методика обучения пользователей (в т.ч. по ИБ)	— Объяснять цели и принципы защиты информации пользователям — Работать в ИБ-проектных командах— Вести документацию и коммуникацию	— Подготовка презентаций и инструкций— Проведение мини-тренингов по ИБ— Командное взаимодействие в ходе внедрения политики безопасности

В результате освоения дисциплины студент преобретет:

Общие знания

- Основные понятия и принципы информационной безопасности: конфиденциальность, целостность, доступность.
- Виды угроз и уязвимостей информационных систем, их классификация.
- Основные методы и средства защиты информации: организационные, программные, технические.
- Модели и механизмы управления доступом (дискреционная, мандатная, ролевая модели).
- Нормативно-правовая база в области ИБ (ФЗ «О персональных данных», ISO/IEC 27001, ГОСТы и др.).
- Архитектура и элементы защищённых информационных систем.
- Основы криптографической защиты информации.

- Подходы к анализу рисков и инцидентов информационной безопасности.
- Роль пользователей, администраторов и руководства в обеспечении ИБ.

Общие умения

- Идентифицировать угрозы и оценивать уязвимости ИС.
- Применять базовые методы защиты информации (антивирусы, брандмауэры, пароли, резервное копирование и др.).
- Разрабатывать и реализовывать простейшие политики информационной безопасности.
- Работать с нормативными документами и использовать их в профессиональной деятельности.
- Анализировать инциденты ИБ и предлагать корректирующие меры.
- Обосновывать выбор технических и программных средств защиты.
- Формировать рекомендации для пользователей по безопасной работе в ИС.
- Участвовать в разработке проектных решений по ИБ.

Общие навыки

- Работа с защитными программами: антивирус, фаервол, средства шифрования, контроль доступа.
- Настройка базовых параметров безопасности в операционных системах и сетях.
- Использование онлайн- и оффлайн-инструментов для проверки уязвимостей.
- Оформление технической и организационной документации по ИБ.
- Проведение инструктажей и демонстрация базовых практик безопасного поведения в ИТ-среде.
- Работа в команде по обеспечению и аудиту информационной безопасности.

7. Образовательные технологии

Изучение дисциплины предполагает использование традиционных способов коллективного обучения – *лекций, лабораторных занятий, индивидуальных заданий с последующей отчетностью.*

Применяемые информационные технологии: *лекции в форме презентаций, обучающие и тестирующие программы, электронные учебники.*

Оценочные средства для текущего контроля успеваемости, рубежного контроля по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы бакалавров:

- **формой текущего контроля знаний студентов (аудиторные занятия)** *является контроль посещения лекционных и практических занятий, активность студентов на практических занятиях. Каждый из двух текущих контролей оценивается по* ***30 баллов.***

формой текущего контроля знаний студентов (внеаудиторные занятия) *является контроль СРСП, участие в НИРС (выступление на студенческой конференции, публикация статей)*

- **формой итогового контроля знаний и умений** бакалавров **по курсу** *является экзамен.*

Текущий и рубежный контроль. Студенты после выполнения соответствующих (первому или второму модулю) практических и лабораторных работ допускаются к рубежному контролю. Каждый из двух рубежных контролей (модулей) оценивается по **30** балльной шкале.

Итоговый контроль. Итоговый контроль реализуется в форме защиты собственно созданных программ (в виде компьютерного тестирования) и оценивается по **30** балльной шкале.

Правила оценивания рубежного и итогового контроля.

8 Критерий оценки знаний студентов на экзамене

Выставление оценок на экзаменах осуществляется на основе принципов объективности, справедливости, всестороннего анализа качества знаний студентов, и других положений, способствующих повышению надежности оценки знаний обучающихся, и устранению субъективных факторов.

В соответствии с действующими нормативными актами и рекомендациями Министерства образования и науки КР устанавливаются следующие критерии выставления оценок на экзаменах:

- ***оценка "отлично"*** выставляется студенту, который обнаружил на экзамене всестороннее, систематическое и глубокое знание учебно-программного матери-ала, умение свободно выполнять задания, предусмотренные программой, который усвоил основную литературу и ознакомился с дополнительной литературой, рекомендованной программой. Как правило, оценка "отлично" выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины и их значений для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

- ***оценка "хорошо"*** выставляется студенту, который на экзамене обнаружил полное знание учебно-программного материала, успешно выполнил предусмотренные в программе задания, усвоил основную

литературу, рекомендованную в программе. Как правило, оценка "хорошо" выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному выполнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности;

- ***оценка "удовлетворительно"*** выставляется студенту, обнаружившему знание основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, предусмотренных программой, который ознакомился с основной литературой, рекомендованной программой. Как правило, оценка "удовлетворительно" выставляется студентам, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя;

- ***оценка "неудовлетворительно"*** выставляется студенту, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не ознакомившемуся с основной литературой, предусмотренной программой, и не овладевшему базовыми знаниями, предусмотренными по данной дисциплине и определенными соответствующей программой курса (перечень основных знаний и умений, которыми должны овладеть студенты, является обязательным элементом рабочей программы курса).

8.1. Оценка знаний (академической успеваемости) осуществляется по 100 балльной системе (шкале) следующим образом:

30 балльная система	**100 балльная система**	**Оценка по буквенной системе**	**Цифровой эквивалент оценки по GPA**	**Оценка по традиционной системе**
26 - 30	87 – 100	A	4,0	Отлично
24 - 25	80 – 86	B	3,33	Хорошо
22 - 23	74 – 79	C	3,0	
20 - 21	68 - 73	Д	2,33	Удовлетворительно
18 - 19	60 – 67	E	2,0	
9 - 17	31 - 60	FX	0	Неудовлетворительно
0 - 8	0 - 30	F	0	

8.2. Технологическая карта дисциплины

Всего	Ауд. часы	СРС, СРСП	1-модуль (90 ч., 30 б.)				2-модуль (90 ч., 30 б.)				Итоговый контроль (ЖТ) (30 б.)				Поо	Всег о
			Ауд. ч.		СРС	Рубе	Ауд. ч.		СРС	Рубе	Лек	Лаб орат	СРС	Ито		
			Лекция	Практические			Лекция	Практические								
90	45	45	15	30	45		15	30	45							
Баллы			**30**	**30**	**30**	**30 б.**	**30**	**30**	**30**	**30 б.**	**30**	**30**	**30**	**30 б**	**10 б**	
Итоги модулей			ТК=(Лек+Лаб+ +СРС)/3, М1=(ТК1+ТК2+ +РК1)/3				ТК=(Лек+Лаб+ +СРС)/3, М2=(ТК3+ТК4+ +РК2)/3				ИК=(Лек+Лаб+ +СРС)/3, Экз=М1+М2+ИК+П					**100**

9. Тематический план и содержание учебной дисциплины «Базы данных»

	Наименование тем лекционных занятий	Кол-во кр О\О	Кол-во кр З\О
1.	**Лекция 1.** Введение в информационную безопасность Понятие информации и информационных процессов Информационные ресурсы и их ценность Определение и цели информационной безопасности Основные объекты защиты	2	2
2.	**Лекция 2.** Принципы и модели информационной безопасности Конфиденциальность, целостность, доступность Триада CIA и расширенные принципы (аутентичность, подотчётность, отказоустойчивость)	2	2

	Модели угроз и нарушителей		
3.	**Лекция 3.** Классификация угроз и уязвимостей Виды угроз: внутренние, внешние, случайные, преднамеренные Уязвимости программного, аппаратного и организационного характера Методы выявления и анализа уязвимостей	2	2
4.	**Лекция 4.** Правовые и нормативные основы ИБ Законодательство РФ и КР в области ИБ (например, ФЗ-152, ФЗ-149) Международные стандарты (ISO/IEC 27001, GDPR) ГОСТы по защите информации, сертификация и лицензирование	2	2
5.	**Лекция 5.** Политика и организационные меры обеспечения ИБ Политика информационной безопасности в организации Регламенты, инструкции, инструкции по доступу и разграничению прав Организация службы ИБ, роли и ответственности	2	2
6.	**Лекция 6.** Криптографические методы защиты информации Основы криптографии: симметричные и асимметричные алгоритмы Электронная подпись и хеш-функции Практическое применение: TLS, HTTPS, PGP	2	СРС
7.	**Лекция 7.** Идентификация, аутентификация и управление доступом Методы идентификации и аутентификации (пароли, биометрия, токены) Модели управления доступом: DAC, MAC, RBAC Примеры систем авторизации и контроля	2	2
8.	**Лекция 8.** Технические средства защиты информации Аппаратные средства защиты (межсетевые экраны, СКЗИ, модули TPM) Антивирусные и антишпионские средства Защита каналов связи	2	2

9.	**Лекция 9.** Программные средства обеспечения безопасности Антивирусы, файерволы, средства резервного копирования Средства обнаружения и предотвращения вторжений (IDS/IPS) Средства мониторинга и логирования	2	2
10.	**Лекция 10.** Безопасность операционных систем Механизмы защиты ОС (Windows, Linux) Настройка политик безопасности Средства управления обновлениями и правами доступа	2	СРС
11.	**Лекция 11.** Сетевая безопасность и защита передачи данных Сетевая архитектура и уязвимости Протоколы безопасности (VPN, IPsec, SSL/TLS) Межсетевые экраны, NAT, фильтрация трафика	2	2
12.	**Лекция 12**. Безопасность веб-приложений Типовые атаки: XSS, SQL-инъекции, CSRF OWASP Top 10 Средства защиты и практики безопасной разработки	2	СРС
13.	**Лекция 13.** Анализ рисков и инцидентов ИБ Методики анализа и оценки рисков Методы реагирования на инциденты Построение системы управления инцидентами	2	СРС
14.	**Лекция 14.** Аудит и оценка эффективности ИБ Цели и принципы аудита ИБ Проведение проверок и внутренний контроль Метрики эффективности системы ИБ	2	СРС
15.	**Лекция 15.** Современные вызовы и тенденции в области ИБ Киберпреступность и социальная инженерия Безопасность в облаках и мобильных платформах Перспективы развития систем защиты и искусственный интеллект в ИБ	2	2
		30	**20**

	Наименование тем практических занятий	Кол-во кр О\О	Кол-во кр З\О
1.	Анализ и классификация угроз информационной безопасности – Работа с реальными кейсами инцидентов и их классификация по источникам и воздействию.	2	2
2.	Идентификация уязвимостей в программном обеспечении и сетях – Использование сканеров уязвимостей (например, Nessus или OpenVAS).	2	2
3.	Разработка и анализ политики информационной безопасности для организации – Проектирование структуры и основных разделов документа.	2	СРС
4.	Работа с нормативно-правовыми документами в сфере ИБ – Анализ требований ФЗ-152, ISO/IEC 27001, ГОСТ Р и др.	2	2
5.	Работа с нормативно-правовыми документами в сфере ИБ – Анализ требований ФЗ-152, ISO/IEC 27001, ГОСТ Р и др.	2	СРС
6.	Настройка межсетевого экрана (Firewall) – Создание правил фильтрации трафика в Windows или Linux iptables.	2	СРС
7.	Применение антивирусного ПО и проверка на вредоносные объекты – Практика с Kaspersky, Dr.Web, ClamAV и анализ отчётов сканирования	2	СРС
8.	Создание и проверка паролей. Методика подбора и защиты – Работа с генераторами паролей, проверка стойкости.	3	2
9.	Настройка резервного копирования и восстановление данных – Создание резервных копий и имитация восстановления системы.	4	СРС

10.	Применение криптографических средств защиты информации – Генерация ключей, шифрование/расшифровка файлов (GPG, VeraCrypt).	2	СРС
11.	Использование цифровой подписи и хеш-функций – Проверка целостности данных и подлинности документов	2	2
12.	Анализ логов безопасности операционной системы – Поиск подозрительной активности в журналах событий.	2	СРС
13.	Выявление атак и несанкционированного доступа в сетях – Использование Wireshark и Snort для анализа сетевого трафика.	2	СРС
14.	Оценка защищённости веб-приложения от типичных атак (OWASP) – SQL-инъекции, XSS и методы защиты (на учебных стендах).	2	СРС
15.	Реагирование на инциденты ИБ: сценарий и отчётность – Разработка плана реагирования, логика действий, составление отчета.	2	2
16.	Анализ рисков ИБ с использованием матрицы угроз – Оценка вероятности и ущерба, построение матрицы.	2	2
17.	Проверка персонального компьютера на соответствие базовым требованиям ИБ – Чек-лист: обновления, пароли, антивирус, фаервол и др.	2	2
18.	Обнаружение шпионского и вредоносного ПО – Практика с утилитами AdwCleaner, Malwarebytes, Process Explorer.	2	2
19.	Построение модели нарушителя и защиты информации в ИС – Выделение объектов защиты, возможных атакующих и методов защиты.	2	2

20.	Создание обучающего мини-курса или инструкции по безопасной работе с ИС – Подготовка видеогида, инфографики или инструкции для пользователей.	4	СРС
		45	**20**

Темы СРС (самостоятельная работа студентов)

Выполняются индивидуально вне аудиторных часов, проверяются в форме отчёта, реферата, презентации или эссе.

№	Тема СРС	Форма выполнения	Ожидаемый результат
1	Обзор действующего законодательства в области ИБ (ФЗ-152, ФЗ-149, GDPR и др.)	Реферат	Аналитический обзор с таблицей требований
2	Сравнительный анализ антивирусных решений (Kaspersky, Avast, Dr.Web и др.)	Презентация	Таблица + выводы о преимуществах/недостатках
3	История и развитие криптографии	Эссе	Краткий исторический обзор и современные применения
4	Обзор OWASP TOP-10 и примеры атак	Мини-отчёт	Перечень уязвимостей + краткие примеры
5	Сравнение стандартов ISO/IEC 27001 и ГОСТ Р 57580	Таблица + вывод	Сравнительная таблица и практические выводы
6	Изучение атак социальной инженерии	Кейс-анализ	2–3 кейса + рекомендации по защите
7	Политика безопасности в образовательной организации	Эссе/наблюдение	Оценка текущей политики ИБ в учебном заведении
8	Актуальные угрозы в киберпространстве (2023–2024 гг.)	Доклад	Подбор и анализ 5–7 актуальных кейсов
9	Этические аспекты хакерской деятельности	Эссе	Рефлексия на тему «этический хакер»
10	Роль человека в системе ИБ	Мнение с аргументами	1–2 страницы + примеры «человеческого фактора»

Темы СРСП (работа под руководством преподавателя)

Выполняется в парах или мини-группах. Защищается очно или в форме публичного представления.

№	Тема СРСП	Формат и цель	Результат
1	Разработка политики информационной безопасности для условной компании	Работа в группе	Готовый документ с разделами и регламентами
2	Анализ инцидента утечки данных	Работа с кейсом	Разбор и план реагирования (мини-презентация)
3	Настройка безопасного канала связи (VPN, SSH, HTTPS)	Практическая работа	Демонстрация + инструкции
4	Моделирование угроз для локальной сети	Совместная работа	Схема + перечень уязвимостей и мер
5	Разработка обучающего буклета по ИБ для сотрудников	Творческое задание	Буклет/плакат/чек-лист
6	Аудит персонального компьютера или учебного стенда	Практика с анализом	Чек-лист и предложения по улучшению
7	Сценарий атаки и защиты от неё (SQL-инъекция, XSS и т.д.)	Интерактивная демонстрация	Видео или пошаговое описание
8	Проведение мини-опроса по теме ИБ среди студентов/преподавателей	Соц. исследование	Результаты в диаграммах + выводы
9	Сравнение систем управления доступом (RBAC, DAC, MAC)	Таблица + презентация	Обоснование выбора модели доступа
10	Подготовка к сертификации по ИБ (ISO, CompTIA, etc.)	Исследование	Краткий гайд по подготовке и содержанию экзамена

10. Учебно-методическое, информационное и материально-техническое обеспечение дисциплины

1. С. И. Макаренко — «Информационная безопасность» (2009)

Описание: Учебное пособие для студентов специальности «Прикладная информатика в экономике». Рассматриваются основы ИБ, угрозы, модели защиты, криптография, организационные меры.

2 В. А. Тихонов, В. В. Райх — «Информационная безопасность: концептуальные, правовые, организационные и технические аспекты» (2006)

Описание: Учебное пособие, посвященное концептуальным, правовым, организационным и техническим аспектам информационной безопасности.

3. Я. С. Гродзенский — «Информационная безопасность» (2020)

Описание: Учебное пособие, рассматривающее основные уровни обеспечения информационной безопасности, включая административный, организационный, законодательный и программно-технический.

4. М. И. Шубинский — «Информационная безопасность для работников бюджетной сферы»

Описание: Пособие, предназначенное для работников бюджетной сферы, охватывающее основы ИБ, организационные меры и практические рекомендации.

5 Основы информационной безопасности – Е. В. Вострецова, 2019. Учебное пособие для студентов направления «Информационная безопасность». Рассматриваются свойства информации как объекта защиты, закономерности создания защищённых информационных систем, принципы обеспечения информационной безопасности государства; дан краткий анализ моделей и политики безопасности, международных стандартов ИБelar.urfu.ru. *Ссылка:* PDF (ElAR УРФУ)elar.urfu.ru.

6 Основы информационной безопасности – С. А. Нестеров, 2014. Учебник СПбПУ (свободный доступ). В пособии системно изложены теоретические основы защиты информации и практические аспекты их реализации: рассматриваются основы криптографии, защита информации в IP-сетях, анализ и управление рисками в сфере ИБ; теоретический материал сопровождается лабораторными работамиelib.spbstu.ru. *Ссылка:* PDF (СПбПУ)elib.spbstu.ru.

7 Информационная безопасность (онлайн-курс) – Лекториум, 2024. Бесплатный дистанционный курс с видеолекциями и заданиями по основам защиты данных в цифровом мирелектorium.tv. Охватывает работу сетей, ОС и баз данных, технологии виртуализации и облачных сервисов, основы безопасного программирования и цифровой гигиены, методы защиты от кибератак и угроз; курс использует практические задания и тесты для закрепления материалалектorium.tv. *Ссылка:* lektorium.tvlektorium.tv.

8 Криптографическая защита информации – Н. А. Гатченко, А. С. Исаев, А. Д. Яковлев, 2012. Учебное пособие ИТМО (СПб). Излагаются основные понятия криптографической защиты информации, блочные и поточные шифры, история развития криптографии и базовые системы шифрования с открытым ключомbooks.ifmo.ru. Рекомендовано студентам и

специалистам по ИБ; снабжено теорией и примерами шифрования. *Ссылка:* PDF (ИТМО)books.ifmo.ru.

Электронный научный архив УрФУ: Основы информационной безопасности : учебное пособие для студентов вуза, обучающихся по укрупненной группе направлений бакалавриата и специалитета 10.00.00 «Информационная безопасность»
https://elar.urfu.ru/handle/10995/73899

Рекомендации по использованию

Для студентов: Рекомендуется начать с учебников Макаренко и Нестерова для получения фундаментальных знаний.

Для преподавателей: Пособия Шаньгина и Гродзенского могут быть полезны при подготовке лекций и практических занятий.

Для самостоятельного изучения: Курс лекций Галатенко и учебник Гафнера предоставляют структурированный материал для самостоятельного освоения дисциплины.

11. Вопросы для подготовки к экзамену

Экзаменационные вопросы

Раздел 1. Основы информационной безопасности

1. Что такое информационная безопасность?
2. Какие объекты подлежат защите в ИС?
3. Перечислите основные свойства защищаемой информации.
4. Что такое конфиденциальность, доступность и целостность?
5. Опишите модель угроз.
6. Что такое политика безопасности информации?
7. Какие основные цели преследует система ИБ?
8. Объясните понятие «доверие к информации».
9. Что такое контроль доступа?
10. Чем отличается ИБ от защиты информации?

Раздел 2. Классификация угроз и уязвимостей

11. Перечислите типы угроз информационной безопасности.
12. Что такое внутренняя и внешняя угроза?
13. Что понимается под уязвимостью информационной системы?
14. Какие категории уязвимостей бывают?
15. Назовите примеры угроз из-за человеческого фактора.
16. Что такое программная уязвимость?
17. Как классифицируются вредоносные программы?
18. Какие признаки указывают на наличие угрозы в ИС?

19. Что такое социальная инженерия? Приведите примеры.
20. Какие последствия могут наступить при реализации угроз?

Раздел 3. Методы и средства защиты информации

21. Перечислите основные методы защиты информации.
22. В чем разница между активной и пассивной защитой?
23. Назовите программные средства защиты информации.
24. Какие существуют технические средства защиты?
25. Что такое организационные меры ИБ?
26. В чем заключается резервное копирование?
27. Что такое система обнаружения вторжений (IDS)?
28. Опишите работу межсетевого экрана (Firewall).
29. Что такое антивирусное программное обеспечение и как оно работает?
30. Какие меры применяют для физической защиты информации?

Раздел 4. Криптографическая защита информации

31. Что такое криптография и в чём её назначение?
32. Назовите основные цели криптографической защиты информации.
33. В чём разница между симметричным и асимметричным шифрованием?
34. Приведите примеры симметричных алгоритмов шифрования.
35. Приведите примеры асимметричных алгоритмов.
36. Что такое электронная цифровая подпись (ЭЦП)?
37. В каких случаях используется ЭЦП?
38. Что такое хеш-функция и для чего она нужна?
39. В чём суть криптографического протокола?
40. Назовите основные этапы процесса шифрования и расшифровки данных.

Раздел 5. Сетевые технологии и защита сетей

41. Какие угрозы характерны для локальных и глобальных сетей?
42. Что такое VPN и как он защищает данные?
43. В чём различие NAT и PAT в сетевой безопасности?
44. Какие функции выполняет межсетевой экран?
45. Что такое IDS и IPS?
46. Как защищаются беспроводные сети Wi-Fi?
47. Какие протоколы безопасной передачи данных вы знаете (TLS, IPsec и др.)?
48. Объясните работу SSL-сертификата.

49. Какие способы существуют для фильтрации трафика?
50. Как осуществляется защита от DDoS-атак?

Раздел 6. Правовые и нормативные основы ИБ

51. Назовите законы РФ, регулирующие защиту информации.
52. Что такое ФЗ-152 и какие данные он защищает?
53. Объясните значение ФЗ-149 «Об информации».
54. Какие виды ответственности предусмотрены за нарушение ИБ?
55. Что такое коммерческая тайна и как она защищается?
56. Назовите международные стандарты ИБ (ISO/IEC 27001 и др.).
57. Что включает ГОСТ по защите информации?
58. В чём назначение документа «Политика информационной безопасности»?
59. Что такое аудит информационной безопасности и кто его проводит?
60. Какие обязанности по ИБ лежат на сотрудниках организации?

Раздел 7. Управление доступом и аутентификация

61. Что такое идентификация и аутентификация?
62. Перечислите основные методы аутентификации пользователей.
63. Что такое двухфакторная аутентификация (2FA)?
64. Опишите модель управления доступом DAC.
65. Что такое мандатная модель (MAC)?
66. В чём особенность ролевой модели управления доступом (RBAC)?
67. Как назначаются права доступа в операционных системах?
68. Что такое принцип наименьших привилегий?
69. Как осуществляется аудит доступа?
70. Что такое список контроля доступа (ACL)?

Раздел 8. Безопасность операционных систем и программного обеспечения

71. Какие механизмы защиты предусмотрены в ОС Windows?
72. Какие механизмы безопасности реализованы в Linux?
73. Что такое политика безопасности ОС?
74. Назовите системные уязвимости, характерные для Windows.
75. Какие меры применяются для обновления и защиты ОС?
76. Что такое патч и зачем он нужен?
77. Что такое доверенная загрузка (Secure Boot)?
78. Какие принципы безопасной разработки программного обеспечения существуют?
79. Что такое «zero-day» уязвимость?

80. Как обеспечивается контроль целостности ПО?

Раздел 9. Социальная инженерия и поведенческие угрозы

81. Что такое социальная инженерия?
82. Какие основные виды атак с использованием социальной инженерии вы знаете?
83. Что такое фишинг и как его распознать?
84. Приведите примеры атак через телефон или мессенджеры.
85. Как можно защитить сотрудников от социальной инженерии?
86. Что такое «pretexting» и как это используется в атаках?
87. Почему важно обучать персонал основам ИБ?
88. Что такое «shoulder surfing» и как от него защититься?
89. Какова роль человеческого фактора в инцидентах ИБ?
90. Какие меры минимизируют поведенческие риски в организации?

Раздел 10. Оценка рисков и реагирование на инциденты

91. Что такое риск в контексте информационной безопасности?
92. Как рассчитывается уровень риска (формула)?
93. Перечислите этапы управления рисками.
94. Что такое актив, угроза и уязвимость в контексте ИБ-риска?
95. В чём разница между качественным и количественным анализом рисков?
96. Какие существуют методы снижения рисков?
97. Что такое план реагирования на инциденты ИБ?
98. Что включает в себя процедура расследования инцидента?
99. Кто отвечает за принятие решения в случае критического инцидента?
100. Что такое журнал инцидентов и как его вести?

Раздел 11. Аудит, контроль и мониторинг

101. Что такое аудит информационной безопасности?
102. Какие цели преследует аудит ИБ?
103. В чём разница между внутренним и внешним аудитом?
104. Какие документы подлежат проверке в ходе аудита ИБ?
105. Какие существуют методы контроля эффективности защиты информации?
106. Что такое непрерывный мониторинг (SIEM)?
107. Назовите ключевые индикаторы эффективности системы ИБ (KPI).
108. Что такое план аудита?
109. Какие последствия могут быть при отсутствии аудита ИБ?

110. Каковы типичные ошибки при проведении аудита ИБ?

Раздел 12. Современные вызовы и облачные технологии

111. В чём состоят современные угрозы ИБ в условиях цифровизации?
112. Какие риски характерны для облачных вычислений?
113. Что такое SaaS, PaaS и IaaS в контексте ИБ?
114. Какие механизмы защиты используются в облачных платформах?
115. Что такое утечка данных (Data Leakage)?
116. Каковы угрозы при использовании мобильных устройств в работе?
117. Что такое BYOD и как обеспечить безопасность в этой модели?
118. Какие вызовы несут технологии IoT (интернета вещей)?
119. В чём опасность искусственного интеллекта в контексте ИБ?
120. Что такое киберустойчивость (cyber resilience)?

Раздел 13. Документация и регламенты по ИБ

121. Какие документы входят в состав политики информационной безопасности организации?
122. Что такое регламент доступа и зачем он нужен?
123. Какие разделы должна содержать политика ИБ?
124. Что такое журнал событий и какие данные он содержит?
125. Как оформляется инцидент ИБ в документации?
126. Какие документы сопровождают криптографическую защиту информации?
127. Что включает в себя акт об уничтожении данных?
128. Зачем нужен приказ о назначении ответственного за ИБ?
129. Как часто должны пересматриваться регламенты по ИБ?
130. Что такое классификация данных и как она оформляется документально?

Раздел 14. Обучение и культура информационной безопасности

131. Зачем обучать сотрудников основам ИБ?
132. Какие темы должны входить в курс внутреннего инструктажа по ИБ?
133. Какие форматы обучения ИБ наиболее эффективны?
134. Что такое фишинговое тестирование персонала?
135. Как формировать культуру ИБ среди сотрудников?
136. Что такое «положительное подкрепление» в контексте ИБ?
137. Как выявить сотрудников с низкой осведомлённостью по ИБ?
138. Какая роль HR-службы в политике ИБ?
139. Что входит в обучение ИБ при приёме на работу?

140. Как оценить эффективность обучающей программы по ИБ?

Раздел 15. Практика, кейсы и анализ реальных ситуаций

141. Опишите типичный сценарий утечки персональных данных.
142. Какие меры позволят быстро локализовать инцидент?
143. Какое ПО используется для анализа журналов событий?
144. Приведите пример успешного предотвращения кибератаки.
145. Какие уроки можно извлечь из кейса с вирусом WannaCry?
146. Что делать в случае компрометации служебной электронной почты?
147. Как правильно реагировать на инцидент шифровальщика (ransomware)?
148. Какие инструменты позволяют выявить несанкционированный доступ?
149. Как проводится внутренняя проверка ИС после инцидента?
150. Как оценить успешность реализации политики ИБ по итогам года?

12. Методические указания для преподавателей дисциплины (модуля)

Цель преподавания дисциплины

Формирование у студентов системного понимания угроз и рисков в информационных системах, освоение методов защиты информации, правовых норм и практических навыков обеспечения информационной безопасности в условиях цифровой трансформации.

Основные задачи преподавателя:

1. **Обеспечить теоретическую базу:**

Донести до студентов ключевые понятия: конфиденциальность, целостность, доступность, уязвимости, криптография, инциденты и т.д.

2. **Организовать практико-ориентированное обучение:**

Практические занятия должны охватывать настройку защиты в ОС, сетях, веб-приложениях, работу с журналами, криптографическими утилитами.

3. **Объяснять правовые аспекты ИБ:**

Особое внимание — законам (ФЗ-152, ФЗ-149), международным стандартам (ISO/IEC 27001), внутренним регламентам.

4. **Ориентировать студентов на современные угрозы и технологии:**

Включать темы кибератак, ИБ в облаках, мобильных устройствах, ИИ и IoT.

5. **Развивать у студентов культуру безопасности:**

Проводить обсуждения, моделирование фишинг-атак, объяснять важность этичного поведения.

Методические рекомендации

- **Использовать кейсы и инциденты:**

Анализировать реальные ситуации (например, утечки данных, вирусы типа WannaCry, DDoS-атаки).

- **Применять интерактивные методы обучения:**

Тесты, симуляции, лабораторные, работа в группах.

- **Оценка знаний:**

Использовать смешанные формы контроля:
– текущий (тесты, опросы, выполнение практики),
– рубежный (экзамен, защита проекта или отчета),
– итоговый (контрольный тест, кейс-анализ, рефлексия).

- **Формировать отчётность по лабораторным:**

Каждый практикум должен завершаться отчётом со скриншотами, выводами и ответами на контрольные вопросы.

Структура занятий (рекомендуемая)

- **Лекции** — 30% времени. Теория с примерами.
- **Практические работы** — 50%. Конфигурация ОС, firewall, VPN, IDS, шифрование.
- **СРС и СРСП** — 20%. Индивидуальные и групповые задания, мини-проекты, рефераты.

Рекомендуемые ресурсы

- **Учебники:**

– С. И. Макаренко «Информационная безопасность»
– С. А. Нестеров «Основы ИБ»
– ISO/IEC 27001, ГОСТ Р 57580

- **Программы:**

– Wireshark, GnuPG, OpenVAS, ClamAV, VeraCrypt

- **Онлайн-курсы:**

– Лекториум, Stepik, Национальная платформа открытого образования

График проведенных практических занятий

	Дата проведения лекционного занятия по расписанию	**Дата проведения практического занятия по расписанию**	**Дата проведения по расписанию СРСП**
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			