МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

Нарынский государственный университет им. С.Нааматова

Аграрно-технический факультет

“СОГЛАСОВАНО”
Начальник учебного управления
Усубалиева Ж.Ж. _____
«_5_» _09_____20_25_г.

“УТВЕРЖДАЮ”
Проректор по учебной работе
Омурова К.О._____
«_5_» _09_____20_25_г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

По дисциплине: **«Информационная безопасность»**
Цикл дисциплины: профессиональный
Направление подготовки 710300: - Информатика и вычислительная техника
Профиль подготовки: Автоматизированные системы обработки информации и управления
Форма обучения: очная

Нарын-20__г.

Рабочая учебная программа составлена на основе стандарта утвержденного МОиН КР. 21-сентября 2021 г. №1578/1 и учебного плана по данному направлению, утвержденному приказом НГУ им. С.Нааматова от 30.06.2022 г., протокол № 10/51

Программу составила:

И.о.доцента кафедры, к.ф-м.н. Кулманбетова С.М. _____

Рассмотрена и одобрена на заседании кафедры Информационные технологии от «14» 01 2026 г., протокол № 6

Заведующий кафедрой,
к.п.н. _____ Бейшеналиева У.У.

Рассмотрена и одобрена на заседании совета факультета от

«15» 01 2026 г., протокол № 6

Декан _____ А.Макеев

АННОТАЦИЯ

Рабочая программа для студентов направления - «Информатика и вычислительная техника» составлена в соответствии с учебным планом по направлению и профилю подготовки.

Общая трудоемкость дисциплины

Семестр	Кредит	Общ.кол.часов	Аудитор.занятия			СРС	отчетность
			Лек	пр	лб		
4	4	120	24		36	60	экзамен

1.1. Дисциплина **«Информационная безопасность»** входит в цикл специальных дисциплин учебного плана - «Информатика и вычислительная техника» Дисциплина изучается на 2 курсе в 4 семестре.

2. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью данной дисциплины является обзор современных проблем в сфере информационной безопасности в информационных системах, а также обзор направлений развития программы информационной безопасности Кыргызской Республики

Задачами дисциплины являются:

- Знаний о современных автоматизированных системах, об угрозах информационной безопасности и о методах и средствах обеспечения информационной безопасности;
- Умений выявлять угрозы информационной безопасности, использовать нормативно-правовые документы по ЗИ, использовать методы и средства обеспечения ИБ и проводить обследование организаций;
- Навыков определения угроз ИБ, приемами разработки политики безопасности предприятия и навыками использования методов и средств обеспечения ИБ;

Для эффективного изучения теоретической части дисциплины **«Информационная безопасность»** необходимо:

♣ построить работу по освоению дисциплины в порядке, отвечающем изучению основных этапов, согласно приведенным темам лекционного материала;

♣ систематически проверять свои знания по контрольным вопросам и тестам;

♣усвоить содержание ключевых понятий;

♣ активно работать с основной и дополнительной литературой по соответствующим темам;

♣ регулярно консультироваться с преподавателем, ведущим изучаемую дисциплину.

Для эффективного изучения практической части дисциплины **«Информационная безопасность»** настоятельно рекомендуется:

♣ систематически выполнять подготовку к лабораторно-практическим занятиям по предложенным преподавателем темам; своевременно выполнять практические задания.

В результате изучения дисциплины студент должен:

Уметь:

- Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности
- Применять основные правила и документы защиты информации в Кыргызской Республике
- Классифицировать основные угрозы безопасности информации

Знать:

- Сущность и понятие информационной безопасности, характеристику ее составляющих
- Место информационной безопасности в системе национальной безопасности страны
- Источники угроз информационной безопасности и меры по их предотвращению

- Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи
- Современные средства и способы обеспечения информационной безопасности.

Владеть:

- техническими средствами и методами защиты информации;
- методами применения криптографических средств защиты информации;
- методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Пререквизиты

Данная дисциплина относится к вариативной части профессионального цикла. Она является неотъемлемой частью профессионального образования студента. Для освоения данной дисциплины требуются знания, полученные в ходе изучения следующих дисциплин:

Код	Наименование дисциплины	Семестр	Трудоемкость в кредитах
Б1.2.2.	Информатика	1	8
Б1.3.2.	Архитектура и организация ПК	2	4

Постреквизиты

Полученные знания могут быть использованы для выполнения выпускной квалификационной работы.

4. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4.1. Компетенции, формируемые в рамках дисциплины «Информационная безопасность»

Код	Содержание компетенции		Результат обучения
ИК-2	Способен приобретать и применять новые знания с использованием информационных технологий для решения сложных проблем в области работы и обучения	Знать	Методы, способы и средства получения, хранения и обработки информации;
		Уметь	Использовать источники экономической, управленческой и социальной информации
		Владеть	Навыками применения современных методов сбора, обработки и анализа данных
ПК-2	способен выбирать методы и средства измерения эксплуатационных характеристик объектов профессиональной деятельности	Знать	способен использовать нормативно правовые документы, международные и отечественные стандарты в

			области ИС и технологий, в том числе сферу информационной безопасности;
		Уметь	Ориентироваться в сфере законодательства и нормативных правовых актов для ИТ; Использовать правовые нормы в сфере информационной безопасности;
		Владеть	Навыками поиска необходимых нормативных и законодательных документов и навыками работы с нивi в области ИС (в том числе информационной безопасности)

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Структура учебной дисциплины

Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	120
Обязательная аудиторная учебная нагрузка (всего)	60
в том числе:	
лекции	24
практические занятия	
лабораторные занятия	36
Самостоятельная работа обучающегося (всего)	60
в том числе:	
составление отчётов по практическим занятиям	25
составление презентаций, рефератов, сообщений	25
подготовка к занятиям	10
Итоговая аттестация: экзамен	

5.2. Содержание учебной дисциплины

Раздел 1. Информационная безопасность, основные понятия и определния. Защита информации. Безопасность информации (данных). Архитектурная безопасность.

Раздел 2. Законодательство об информационных правоотношениях. Уровни правового обеспечения информационной безопасности информации и информационной безопасности предприятия

Радел 3. Международные стандарты информационного обмена. Понятие угрозы. Концепция информационной безопасности

Тематический план, отражающий содержание дисциплины (темы лекций), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице:

№	Наименование разделов и тем		
		Лк	СРС
1	История становления теории информационной безопасности	2	4
2	Информация как объект защиты. Классификация угроз ИБ. Злоумышленники: хакеры, инсайдеры, киберпреступность. Мотивация и цели атак	2	4
3	Государственная политика КР по информационной безопасности. Нормативно-правовая база ИБ	2	4
4	Комплексный подход к обеспечению безопасности.	2	4
5	Классификация криптографических систем	2	4
6	Аутентификация и идентификация, основные понятия	2	6
7	Защита операционных систем. Аутентификация, авторизация, аудит. Управление учетными записями и политиками безопасности Использование алгоритмов шифрования	2	6
8	Виды возможных нарушений ИС. Особенности нарушений ИС в конкретных предметных областях Резервное копирование и аварийное восстановление (DRP). Политики бэкапа. Инцидент-менеджмент: что делать при атаке?	2	6
9	Обзор международных стандартов информационной безопасности. Современные тенденции: облачная безопасность (Shared Responsibility Model), мобильная безопасность, DevSecOps	2	4
10	Понятие о вредоносных программах. Компьютерные вирусы	2	6
11	Защита на уровне сети. Фаерволлы (межсетевые экраны). Принципы работы, типы (packet filtering, stateful). VPN. Методы защиты информации в компьютерных сетях. Обеспечение информационной безопасности в Интернет	2	6
12	Таксономия нарушений информационной безопасности ВС и причины обусловливающие их сушествование. Оценка надежности защитных механизмов Социальная инженерия. Фишинг, вишинг, претекстинг. Методы защиты пользователей и сотрудников.	2	6
	Итого:	**24**	**60**

	Темы лабораторных занятий	Кол.часов
1	Настройка базовых правил фаервола (iptables/Windows Firewall). Создание простого VPN-туннеля (WireGuard/OpenVPN)	2
2	Классификация защищаемой информации по видам тайны и степеням конфиденциальности. Разбор кейсов утечек данных из облаков. Обсуждение модели ответственности провайдера vs. клиента	4

3	Определение угроз объекта информатизации и их классификация. Настройка политик паролей и прав доступа в Windows/Linux. Анализ журналов событий на предмет подозрительной активности.	2
4	Изучение нормативно-правовых актов КР по информационной безопасности	2
5	Изучение международных нормативно-правовых систем и документов по информационной безопасности	2
6	Выбор мер защиты информации для автоматизированного рабочего места.	2
7	Неформальная модель нарушителя, классификация нарушителей. Оценка уязвимости системы. Анализ вредоносных образцов в песочнице (Any.Run, виртуальная среда). Изучение поведения malware и сигнатур	4
8	Основы безопасности IoT-устройств и промышленных систем (КТС). Угрозы для «умного дома» и АСУ ТП	4
9	Изучение ППП систем криптографической защиты информации, классическая криптография и распределение ключей. Поиск и эксплуатация базовых уязвимостей на учебном веб-приложении (DVWA, WebGoat): SQL-инъекция, XSS	2
10	Асимметричное шифрование. Изучить: конфиденциальность, целостность, доступность (CIA-триада).	2
11	Электронная цифровая подпись (ЭЦП)	2
12	Криптосистема операционной системы Windows. Этика хакера. White Hat, Grey Hat, Black Hat. Ответственное раскрытие уязвимостей (Bug Bounty). Профессии в ИБ	2
13	CryptoAPI: шифрование и дешифрование в CryptoAPI, ЭЦП в проектах на CryptoAPI	2
14	Практическое применение криптографии с открытым ключом. Пакет PGP	4
	Итого:	**36**

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ.

В процессе освоения дисциплины «Информационная безопасность» используются следующие образовательные технологии:

1. Стандартные методы обучения:
   – лекции;
   – семинары;
   – письменные или устные домашние задания;
   – консультации преподавателей;
   – самостоятельная работа студентов, в которую входит освоение теоретического материала, подготовка к семинарам, выполнение указанных выше письменных работ.
2. Методы обучения с применением интерактивных форм образовательных технологий:
   – интерактивные лекции;
   – анализ деловых ситуаций на основе кейс-метода и имитационных моделей;
   – круглые столы;
   – обсуждение подготовленных студентами рефераты;
   – групповые дискуссии и проекты;

7. ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ,

ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ И РЕАЛИЗУЕМЫХ В УЧЕБНОЙ ДИСЦИПЛИНЕ КОМПЕТЕНЦИЙ.

В соответствии с требованиями ГОС ВПО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине созданы фонды оценочных средств (Приложение 1).

8. ОРГАНИЗАЦИЯ КОНТРОЛЬНО-ОЦЕНОЧНОЙ ДЕЯТЕЛЬНОСТИ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Успешное освоение дисциплины предполагает активное, творческое участие обучающегося на всех этапах ее освоения путем планомерной, повседневной работы. Обучающийся обязан посещать лекции, семинарские, практические и лабораторные занятия (при их наличии), получать консультации преподавателя и выполнять самостоятельную работу. Изучение дисциплины следует начинать с проработки настоящей рабочей программы, методических указаний и разработок, указанных в программе, особое внимание уделить целям, задачам, структуре и содержанию дисциплины. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее основных положений. Тематика лекций определяется настоящей рабочей программой дисциплины.

Лекции – это систематическое устное изложение учебного материала. На них обучающийся получает основной объем информации по каждой конкретной теме. Лекции обычно носят проблемный характер и нацелены на освещение наиболее трудных и дискуссионных вопросов. Предполагается, что:

- оценки «отлично» заслуживает студент, который привел развёрнутые ответы на все вопросы конспектирования с приведением фактов и примеров;
- оценки «хорошо» заслуживает студент, который привел развёрнутые ответы на все вопросы конспектирования с незначительным числом фактов и примеров;
- оценки «удовлетворительно» заслуживает студент, который привел ответы на все вопросы конспектирования;
- оценки «неудовлетворительно» заслуживает студент, который не предоставил конспект.

Целью практических и лабораторных занятий является формирование у обучающихся умений и навыков применения теоретических знаний в реальной практике решения задач; восполнение пробелов в пройденной теоретической части курса. Семинарские, практические и лабораторные занятия в равной мере направлены на совершенствование индивидуальных навыков решения теоретических и прикладных задач, выработку навыков интеллектуальной работы, а также ведения дискуссий. Для успешного участия в семинарских, практических и лабораторных занятиях обучающемуся следует тщательно подготовиться. Основной формой подготовки обучающихся к практическим (лабораторным) занятиям является самостоятельная работа с учебно-методическими материалами, научной литературой, статистическими данными и т.п.

Обучающимся рекомендуется систематически отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки. При проведении промежуточной аттестации обучающегося учитываются результаты текущего контроля, проводимого в течение освоения дисциплины.

Примерные критерии оценки СРС

Параметры оценивания	Кол-во баллов
1.Понимание содержания СРС (реферата, эссе и др.), через четкую формулировку целей и задач ее.	10-20
Наличие плана выполнения письменной работы (реферата, эссе и др.).	5-10
Наличие и формулировка выводов, обобщений	10
Грамматика и стилистика письменной работы (реферата, эссе и др.)	5-10
Оформление письменной работы (реферата, эссе и др.)	10
Итого	**24-40**

9. ВИДЫ И ФОРМЫ ОТРАБОТКИ ПРОПУЩЕННЫХ ЗАНЯТИЙ

Пропущенные занятия студент отрабатывает до начала модуля. Студент, пропустивший лекционное занятие, обязан предоставить конспект соответствующего раздела учебной литературы (основной и дополнительной) по рассматриваемым вопросам в соответствии с программой дисциплины. Студент, пропустивший практическое занятие, отрабатывает его в форме реферативного конспекта соответствующего раздела учебной литературы (основной и дополнительной) по рассматриваемым на практическом занятии вопросам в соответствии с программой дисциплины или в форме, предложенной преподавателем. На лекциях преподаватель рассматривает вопросы программы курса, составленной в соответствии с государственным образовательным стандартом. Преподаватель, по своему усмотрению, некоторые вопросы выносит на самостоятельную работу студентов, в этом случае студенту выдается список литературы или материалы, включенные в учебно-методический комплекс дисциплины.

10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1.Е. В.Вострецова, Основы информационной безопасности. Екатеринбург, 2019.
2. Научно-методические основы обеспечения безопасности защищаемых объектов Автор: Ю.Б. Михайлов, Издательство: Горячая Линия - Телеком, ISBN 978-5-9912-0485-9; 2015 г.
3. Безопасность компьютерных сетей Автор: В.Г. Олифер, Н.А Олифер, Издательство: Горячая Линия - Телеком, ISBN 978-5-9912-0420-0; 2015 г.
4. Методы оценки несоответствия средств защиты информации Авторы: А.С. Марков, В.Л. Цирлов, А.В. Барабанов, Издательство: Радио и связь, ISBN 5-89776-015-2; 2012 г.
5. Информационная безопасность открытых систем Автор: Д.А. Мельников, Издательство: Флинта, ISBN 978-5-02-037923-7; 2013 г.
6. Стандарты информационной безопасности Автор: В. А. Галатенко, Издательство: Интернет-университет информационных технологий, Серия: Основы информационных технологий, ISBN 978-5-9556-0053-6; 2010 г.;

Дополнительная литература

1. Теоретические основы компьютерной безопасности / П.Н. Девянин [и др.].— Москва : Радио и связь, 2000.— 192 с. 4. Бардаев Э.А. Документоведение : учебник для студ. высш. учеб. заведений / Э.А. Бардаев, В.Б. Кравченко.— Москва : Издательский центр «Академия», 2008.— 304 с.
2. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин.— Москва : Горячая линия — Телеком, 2001.— 148 с.
3. Мельников В.В. Безопасность информации в автоматизированных системах / В.В. Мельников.— Москва : Финансы и статистика, 2003.— 368 с.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Реализация программы дисциплины требует наличия компьютерного класса с выходом в сеть Интернет.

Оборудование компьютерного класса:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- персональные компьютеры с программным обеспечением и выходом в сеть Интернет;
- офисные программы: текстовый процессор, табличный процессор, программы создания презентаций, программа для работы с электронной почтой;
- современные антивирусные программные продукты.

Средства обеспечения освоения дисциплины

В процессе изучения дисциплины, студент работает с многочисленными информационными источникам в сети Интернет.

В качестве примеров ссылок на интернет-источники можно привести:

http://intuit.ru

http://lib.ru

Материально-техническое обеспечение дисциплины:

Технические и аудиовизуальные средства (мультимедийный компьютерный класс. интерактивная доска), наличие локальной и глобальной сети.

12. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Целью индивидуальных (самостоятельных) занятий является самостоятельное более глубокое изучение студентами отдельных вопросов курса с использованием рекомендуемой дополнительной литературы и других информационных источников.

Критериями оценки результатов внеаудиторной самостоятельной работы являются:

– уровень освоения учебного материала;

– полнота представлений, знаний и умений по изучаемой теме, к которой относится данная самостоятельная работа;

– обоснованность и четкость изложения ответа на поставленный по внеаудиторной самостоятельной работе вопрос;

– оформление отчетного материала в соответствии с известными или заданными преподавателем требованиями, предъявляемыми к подобного рода материалам.

ТРЕБОВАНИЯ ПО ОФОРМЛЕНИЮ РЕФЕРАТА

1. оформление реферата аналогично оформлению курсовых работ (титульный лист, аннотация, содержание, текст реферата, информационные источники, приложения).

2. объем реферата не менее 10 страниц формата А4, шрифт Times New Roman, кегль 14 пт, междустрочный интервал -1,5, выравнивание текста – по ширине, нумерация страниц в нижнем колонтитуле; 3. на титульном листе указывается: название реферата, Фамилия И.О. исполнителя, факультет, специальность, курс, группа;

4. список использованных источников - не менее 3-х, полное указание выходных данных для книжных и периодических изданий, адреса сайтов с которых заимствован материал, по тексту реферата должны быть ссылки на источники;

5. реферат должен содержать достоверные и актуальные сведения на достаточном научном уровне;

6. реферат, кроме текста (формат .doc), может дополнительно содержать:

– качественные цветные иллюстрации;

– фрагменты программ;

– исполняемые модули;

– фрагменты информационных систем;

– презентации;

– другие материалы, качественно дополняющие основную часть реферата;

Приложение 1.

БАЗА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ «Информационная безопасность»

«Утверждаю»
Зав.кафедрой Бейшеналиева У.У.

«____»_____20__г.

Темы самостоятельных работ студента

1. Эволюция вредоносного ПО: от вирусов до полиморфных программ-вымогателей.
2. Фишинг: методы, психологические основы и современные тенденции.
3. Криптовалюты и безопасность: угрозы для бирж и кошельков.
4. Безопасность беспроводных сетей Wi-Fi: методы взлома WPA2 и защита.
5. Анонимность в интернете: технологии (Tor, VPN) и их ограничения.
6. Биометрическая аутентификация: удобство vs. риски.
7. Уязвимости в цепочке поставок программного обеспечения (Supply Chain Attacks).
8. Кибербуллинг и троллинг: социальные аспекты информационной безопасности.
9. Безопасность умного дома: анализ угроз и реальные случаи взлома.
10. Защита от DDoS-атак: современные методы и сервисы (CDN, scrubbing-центры).
11. Роль искусственного интеллекта в кибербезопасности: для атак и защиты.
12. Deepfake-технологии как угроза информационной безопасности.
13. Безопасность мобильных банковских приложений.
14. Киберпреступность как сервис (Crime-as-a-Service): аренда ботнетов, хакерских инструментов.
15. Правовые аспекты борьбы с киберпреступностью в РФ и мире.
16. Этичный хакинг: суть, методы и легальные рамки деятельности.
17. Анализ громких случаев утечек персональных данных (на примере одной компании).
18. Безопасность в социальных сетях: риски и настройки приватности.
19. Технология блокчейн с точки зрения безопасности.
20. Кибербезопасность в компьютерных играх: читы, кражи аккаунтов, DDoS.
21. «Ошибка человеческого фактора» как главная угроза ИБ в организациях.
22. Безопасность облачных хранилищ данных: сравнительный анализ провайдеров.
23. Методы социальной инженерии на примере кино и литературы.
24. Безопасность систем видеонаблюдения и «умных» камер.
25. Риски и угрозы в сетях 5G.
26. Понятие «цифрового следа» и методы его минимизации.
27. Защита детей в интернете: технические и воспитательные меры.
28. Кибербезопасность в условиях удаленной работы (Remote Work).
29. Анализ рынка антивирусного ПО: механизмы работы и эффективность.
30. Будущее паролей: какие технологии их заменят (FIDO2, пасс-кеи)?

Контрольные вопросы первого модуля

1. Какие методы защиты информации, использовавшиеся в древнее время и в Средние века Вам известны?
2. Покажите связь между уровнем развития общества и технологиями защиты информации.
3. В каких направлениях идет развитие теории информационной безопасности в настоящее время?
4. Каков вклад российских ученых в теорию информационной безопасности?
5. С чем связан возросший интерес к проблемам защиты информации?
6. Каковы отличия формального и неформального подходов к проблемам защиты информации?

7. В чем, на Ваш взгляд, заключаются основные трудности обеспечения информационной безопасности в настоящее время?
8. Каковы правовые понятия в области защиты информации?
9. Что такое защита информации? Информационная безопасность?
10. Охарактеризуйте понятия, связанные с организацией защиты информации.
11. Каковы основные принципы построения систем защиты информации?
12. Что такое комплексный подход к обеспечению информационной безопасности?
13. Каковы основные задачи защиты информации?
14. Докажите, что приведенное множество функций защиты является полным.
15. Какова взаимосвязь различных средств защиты информации? Есть ли среди них приоритетные?
16. Каковы основные средства реализации комплексной системы защиты информации?
17. Что такое информация и каковы уровни ее представления?
18. Перечислите основные носители информации, особенности их использования и защиты.
19. Какими свойствами определяется ценность информации?
20. Какие критерии оценки ценности информации Вы можете предложить?
21. Приведите примеры различной зависимости ценности информации от времени.
22. Что понимается под информационными ресурсами?
23. Что не разрешается относить к информации ограниченного доступа?
24. Что понимается под конфиденциальной информацией?
25. Какие существуют виды тайны?
26. Какое назначение имеет перечень конфиденциальных сведений предприятия
27. Что такое национальная безопасность
28. Что регулирует закон КР «Об информатизации»
29. Что такое конституция
30. Что способствует быстрое развитие ИТ к информационной безопасности
31. Что такое информационная безопасность
32. Перечислите основные составляющие ИБ
33. Что такое угроза ИБ
34. Перечислите классификацию угроз
35. Назовите основные направления и методы реализации угроз
36. Какие меры требуется для защиты ИБ
37. Закон КР «Об информации персонального характера»
38. Какие меры можно выделить на процедурном уровне
39. Перечислите основные направления физической защиты
40. Что являются средствами физической защиты
41. Какие международные стандарты существуют о ИБ
42. Что такое «Оранжевая книга»
43. Механизм безопасности

Контрольные вопросы второго модуля

1. Что такое криптография и для чего используется
2. Дайте определение термину «криптология»
3. История развития криптографии
4. Что такое стеганография
5. Что такое шифр, расшифровка и шифровка
6. Сколько видов шифрования в настоящее время
7. Типы криптосистем
8. Что такое криптоатака и стойкость алгоритмов
9. Что такое аутентификация и для чего используется
10. Что такое идентификация

11. Чем отличается односторонняя аутентификация от двусторонней
12. Что такое парольная аутентификация
13. Как создать пароль, правила и меры предосторожности
14. Что такое биометрические данные
15. Преимущества и недостатки биометрической идентификации
16. Опишите канальное шифрование
17. Что такое сквозное шифрование
18. Сравните канальное и сквозное шифрование
19. Преимущество и недостатки обеих шифрований
20. Что такое шифрование на уровне файла и на уровне драйвера
21. Аппаратное и программное щифрование, преимущества и недостатки
22. Цели применения стандартов информационной безопасности.
23. Охарактеризуйте основные положения Оранжевой книги.
24. Почему в современных стандартах отказываются от единых шкал, характеризующих уровень безопасности?
25. Каковы основные положения Европейских критериев безопасности информационных технологий?
26. Чем отличаются «информационная система» и «продукт информационных технологий»?
27. Для чего вводятся критерии адекватности?
28. Что такое Профиль защиты?
29. В чем особенности Канадских критериев безопасности компьютерных систем?
30. Опишите структуру Общих критериев безопасности информационных технологий.
31. Опишите технологию применения Общих критериев безопасности информационных технологий.
32. Каковы тенденции развития международной нормативной базы в области информационной безопасности?
33. Самостоятельно изучить документ по ссылке http://cbd.minjust.gov.kg/act/view/ru-ru/15479

Контрольные вопросы для самостоятельного изучения

1. Раскройте содержание CIA-триады. Приведите примеры нарушения каждого принципа.
2. Дайте определение угрозе, уязвимости и риску в ИБ. Как они связаны?
3. Перечислите основные классы злоумышленников и их мотивацию.
4. В чем разница между симметричным и асимметричным шифрованием? Плюсы и минусы.
5. Для чего нужна хэш-функция? Приведите примеры использования (пароли, целостность).
6. Объясните принцип работы межсетевого экрана (фаервола). Типы фильтрации.
7. Что такое VPN и какие задачи защиты он решает?
8. Опишите суть атаки «Отказ в обслуживании» (DoS/DDoS). Основные типы.
9. Что такое атака «человек посередине» (MITM)? Как от неё защититься?
10. Назовите основные этапы жизненного цикла вредоносного ПО.
11. В чем отличие вируса, червя и трояна?
12. Что такое социальная инженерия? Опишите три распространенных метода.
13. Что такое SQL-инъекция? Механизм, последствия, способы защиты.
14. Раскройте суть межсайтового скриптинга (XSS). Типы XSS.
15. Для чего нужна политика резервного копирования? Правило 3-2-1.
16. Что такое план аварийного восстановления (DRP)? Ключевые этапы.
17. Какие основные требования к защите ПДн предъявляет Закон о персональных данных в КР?
18. Назовите основные положения стандарта ISO 27001.
19. В чем заключается модель разделенной ответственности в облачной безопасности?
20. Основные угрозы безопасности для IoT-устройств.
21. Что такое DevSecOps? Как интегрируется безопасность в цикл разработки?

22. Опишите различия между White Hat, Grey Hat и Black Hat хакерами.
23. Что такое Bug Bounty программа? Принципы ответственного раскрытия уязвимостей.
24. Перечислите ключевые профессии в сфере ИБ (аналитик, пентестер, SOC-инженер и др.).
25. Для чего нужны системы SIEM? Какой основной принцип их работы?
26. Что такое индикатор компрометации (IoC) и тактика, техника, процедура (TTP)?
27. Опишите базовые меры защиты рабочей станции пользователя.
28. Что такое «песочница» (sandbox) и для чего она используется в ИБ?
29. Каковы, на ваш взгляд, главные тренды и вызовы в ИБ на ближайшие 5 лет?

Тестовые вопросы:

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
- Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
- Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
- несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
- Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
- Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
- органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
- Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:
- Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
- Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы

- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

- Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

- Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой
- Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- Удалить письмо с приложением, не раскрывая (не читая) его