Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
Московский государственный университет имени М.В. Ломоносова
Высшая школа управления и инноваций

УТВЕРЖДАЮ
(и.о.декана)
_____/В.В.Печковская/
«9» июня 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Уровень высшего образования:
Магистратура

Направление подготовки (специальность):
27.04.05 «Инноватика» (3++)

Форма обучения:

очная

Рабочая программа рассмотрена и одобрена
На заседании Совета факультета
(протокол № 3, 9 июня 2021 г.)

Москва 2022

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки / специальности 27.04.03 "Системный анализ и управление" (программа магистратуры), утвержденным приказом МГУ от 22 июля 2011 года № 729 (в редакции приказов МГУ от 22 ноября 2011 года № 1066, от 21 декабря 2011 года № 1228, от 30 декабря 2011 года № 1289, от 22 мая 2015 года № 490, от 30 июня 2016 года № 746, от 30 декабря 2020 года №1376).

Год (годы) приема на обучение: 2021.

I. Цели и задачи учебной дисциплины

Целью изучения дисциплины «Информационная безопасность и защита информации» изучение методологических и алгоритмических основ, стандартов, а также механизмов и сервисов безопасности информационных технологий. Значительное внимание уделяется изучению наиболее важных сервисов и механизмов защиты информации, криптографических алгоритмов и протоколов, проблем информационной безопасности в сети интернет.

Задачами дисциплины являются: изучение основных алгоритмов симметричного шифрования: DES, 3DES, IDEA, ГОСТ 28147, Blowfish, Rijndael, а также режимов их использования; изучение алгоритмов шифрования с открытым ключом: RSA, Диффи-Хеллмана и DSS, изучение принципов распределения открытых ключей, стандарта X.509 третьей версии и принципов создания инфраструктуры открытого ключа, изучение наиболее широко используемых протоколов сетевой безопасности прикладного уровня и протоколов создания виртуальных частных сетей.

II. Место дисциплины в структуре ОПОП ВО

Дисциплина «Разработка программного обеспечения» является дисциплиной по выбору профессионального блока вариативной части программы магистратуры.

Изучение дисциплины базируется на знаниях и умениях, полученных обучающимися в процессе изучения гуманитарных, экономических и IT дисциплин: «Информационные технологии».

Для успешного освоения дисциплины обучающийся должен:

Знать:

— основные понятия и классификацию основных схем структурного программирования;

Уметь:

— работать с информацией в глобальных компьютерных сетях, разрабатывать и реализовывать простейшие алгоритмы на основе поставленного задания, применять в профессиональной деятельности современные языки программирования;

Владеть:

— навыками работы с компьютером как средством управления информацией, разработки алгоритмических и программных решений в области прикладного программирования.

Знания, навыки и умения, полученные при изучении дисциплины «Разработка программного обеспечения» необходимы для прохождения производственной и преддипломной практики, осуществления научно-исследовательской работы и написания выпускной квалификационной работы (магистерской диссертации). Изучается на 2 курсе (3 семестр).

III. Требования к результатам освоения дисциплины

В результате освоения дисциплины должны быть сформированы следующие компетенции:

Код и наименование компетенции	Код и наименование индикатора	Планируемые результаты
Универсальные компетенции		
УК-1. Способен осуществлять критический анализ	**УК-1.1.** Анализирует проблемную ситуацию как	**Знать:** – основные методы

проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий, формулировать научно обоснованные гипотезы, применять методологию научного познания в профессиональной деятельности	систему, выявляя ее составляющие и связи между ними	критического анализа; − методологию системного подхода; **Уметь:** − выявлять проблемные ситуации, используя методы анализа, синтеза и абстрактного мышления; − осуществлять поиск решений проблемных ситуаций на основе действий, эксперимента и опыта; − производить анализ явлений, обрабатывать полученные результатов, делать обоснованные выводы; − определять в рамках выбранного алгоритма вопросы (задачи), подлежащие дальнейшей разработке и предлагать способы их решения; **Владеть:** − технологиями выхода из проблемных ситуаций, навыками выработки стратегии действий; − навыками критического анализа; − навыками применения системного подхода к анализу проблемных ситуаций. − навыками интерпретации полученных данных в ходе анализа проблемной ситуации и формирования обоснованных выводов.

	УК-1.2. Разрабатывает и обосновывает стратегию действий по решению проблемной ситуации на основе системного и междисциплинарных подходов.	**Знать** основные положения разработки стратегии действий по решению проблемной ситуации; **Уметь:** – разрабатывать и обосновывать стратегию действий по решению проблемной ситуации; – использовать системный и междисциплинарные подходы к решению проблемной ситуации; **Владеть** навыками разработки стратегии действий по решению проблемной ситуации на основе системного и междисциплинарных подходов.
	УК-1.3. Использует логико-методологический инструментарий для решения проблемной ситуаций.	**Знать** основные положения использования логико-методологического инструментария; **Уметь** использовать логико-методологический инструментарий для решения проблемной ситуаций; **Владеть** навыками применения

		логико-методологического инструментария для решения проблемной ситуаций.
	УК-1.4. Формулирует научно обоснованные гипотезы, применяет методологию научного познания в профессиональной деятельности.	**Знать:** − основные положения формулирования научно обоснованных гипотез; − методы научного познания; **Уметь:** − формулировать научно обоснованные гипотезы; − применять методологию научного познания в профессиональной деятельности; **Владеть:** − навыками формулирования научно обоснованных гипотез в решении задач профессиональной деятельности; − навыками применения методов научного познания в решении профессиональных задач.
Общепрофессиональные компетенции		
ОПК-1. Способен анализировать и выявлять естественно-научную сущность проблем управления в технических системах на основе положений, законов и методов в области математики, естественных и технических наук	**ОПК-1.1.** Демонстрирует знание законов, естественно-научных и математических методов для использования в профессиональной деятельности в области управления в технических системах.	**Знать:** фундаментальные законы природы и основные физические математические принципы; **Уметь:** применять физические законы и математические методы для решения задач теоретического и прикладного характера в области управления в технических системах; **Владеть:** навыками использования знаний математики, естественных и технических наук при решении

		практических задач в области управления в технических системах;
	ОПК 1.2. Проводит анализ и выявляет естественно-научную сущность проблемы управления в технической системе.	**Знать:** − естественнонаучные методы познания; − методологию научных исследований; **Уметь:** − проводить анализ проблемы и выявлять её естественнонаучную сущность; − применять законы математики, естественных и технических наук для анализа проблемы управления в технической системе; **Владеть** навыками определения естественнонаучной сущности проблемы управления в технической системе.

ОПК-2. Способен формулировать задачи управления в технических системах и обосновывать методы их решения	**ОПК-2.1.** Формулирует задачи управления в технических системах на основе знаний, профильных разделов математических и естественнонаучных дисциплин	**Знать:** фундаментальные разделы, профильные разделы математических и естественнонаучных дисциплин; **Уметь** формулировать задачи профессиональной деятельности на основе знаний, профильных разделов математических и естественнонаучных дисциплин; **Владеть** методами формулирования задач профессиональной деятельности на основе знаний в области математики, естественных и технических наук.
ОПК-3. Способен самостоятельно решать задачи управления в технических системах на базе последних достижений науки и техники	**ОПК-3.1.** Применяет результаты и тенденции последних достижений науки и техники для решения задач в области управления в технических системах	**Знать:** особенности развития последних достижений науки и техники в области управления в технических системах; **Уметь:** – выявлять тенденции технологического развития в наукоемких сферах деятельности; – решать задачи управления в технических системах с использованием современных технологий; **Владеть:** навыками применения современных технологий для решения задачи управления в технических системах.
	ОПК-3.2. Использует фундаментальные знания	**Знать:** общие методы решения базовых задач управления в

	для решения базовых задач управления в технических системах	технических системах; **Уметь:** − применять знания естественных наук для построения математических моделей объектов и процессов; − применять методы и способы решения базовых задач в технических системах; **Владеть** навыками решения базовых задач управления в технических системах.
Профессиональные компетенции		
ПК-2. Способен выявлять и оценивать тенденции технологического развития в наукоемких сферах деятельности, осуществлять технологическое прогнозирование	**ПК-2.1.** Выявляет и оценивает тенденции технологического развития в наукоемких сферах деятельности	**Знать:** − методы построения концептуальных, математических и имитационных моделей; − передовой отечественный и зарубежный опыт в области развития науки и техники; − методы прогнозирования, технико-экономических исследований научно-технических решений и нормативного проектирования инновационных видов продукции и процессов; **Уметь:** − анализировать научную, научно-техническую информацию; − выявлять и оценивать тенденции технологического развития в наукоемких сферах на основе анализа, обобщения и систематизации передового опыта в сфере инноватики по материалам ведущих научных

		журналов и изданий, с использованием электронных библиотек и интернет-ресурсов; – оценивать возможные результаты внедрения передовых технологических решений; **Владеть** навыками подготовки заключений и отзывов на инновационные предложения повышения эффективности в наукоемких сферах деятельности.
	ПК-2.2. Осуществляет технологическое прогнозирование	**Знать** основные положения и методы технологического прогнозирования; **Уметь:** – использовать источники информации для анализа данных, необходимых для составления прогноза; – применять методы анализа данных и построения математических моделей; – применять программные средства планирования, мониторинга, контроля исполнения, формирования прогнозных данных; – выполнять технико-экономический анализ проектных, конструкторских и технологических решений для выбора оптимального варианта реализации инноваций; – прогнозировать тенденции развития науки и техники в профессиональной сфере;

		Владеть навыками формирования прогноза технологического развития.
ПК-9. Способен планировать и осуществлять мероприятия по адаптации организации к изменяющимся условиям рынка с учётом тенденций развития науки и техники, руководить процессом организационных изменений при внедрении новой техники и технологий	**ПК-9.1.** Планирует и осуществляет мероприятия по адаптации организации к изменяющимся условиям рынка с учётом тенденций развития науки и техники	**Знать:** – принципы и основные положения теории решения нестандартных задач, законы эволюции сложных систем, принципы функционального моделирования технических систем и типовые методы их совершенствования; – классификация и основные методы моделирования бизнес-процессов; **Уметь:** – оценивать инновационный потенциал организации; – планировать мероприятия по внедрению и сокращению сроков освоения новой техники и технологии, рациональному использованию ресурсов, повышению эффективности деятельности организации, улучшению качества продукции, совершенствованию организации труда; **Владеть** навыками разработки плана совершенствования организации производства, труда и управления на основе внедрения новейших технических и телекоммуникационных средств.

	ПК-9.2. Руководит процессом организационных изменений при внедрении новой техники и технологий	**Знать:** – современные принципы и технологии менеджмента; – особенности осуществления организационных изменений; – программы (инструменты) корпоративных инноваций; **Уметь:** – оценивать готовность организации к осуществлению организационных изменений и корпоративных инноваций; – анализировать барьеры осуществления организационных изменений и разрабатывать меры по их устранению; – анализировать инновационный потенциал организации и выбирать соответствующие программы (инструменты) корпоративных инноваций; – принимать управленческие решения по осуществлению организационных изменений при внедрении новой техники и технологий; **Владеть** – навыками принятия управленческих решений по осуществлению организационных изменений при внедрении новой техники и технологий; – навыками руководства и организации процесса планирования организационных изменений.

ПК-17. Способен применять современные информационные технологии и технические средства для подготовки, публичного представления и защиты проекта (программы) в виде презентации.	**ПК-17.1.** Применяет современные информационные технологии и технические средства для подготовки презентации проекта (программы)	**Знать:** – технологии подготовки и проведения презентаций; – методы создания рекламных текстов; – основы работы с программными и техническими средствами по подготовке презентаций; **Уметь:** – составлять информационных материалы; – подготавливать презентации с использованием технических средств; **Владеть** навыками подготовки презентации проекта (программы).
	ПК-17.2. Публично представляет и защищает презентацию проекта (программы)	**Знать:** – правила аргументации и обоснования проекта (программы); – приёмы публичного выступления; **Уметь:** – убеждать собеседника; – проводить публичные презентации с использованием современных информационных технологий и технических средств; – проводить переговоры; – организовывать встречи, совещания, презентация в рамках реализации проекта (программы);

		Владеть навыками публичной защиты основных положений проекта (программы).
СПК-3. Способен применять методы анализа данных для решения профессиональных задач посредством применения современных инструментальных и программных средств	**СПК-3.1.** Применяет методы анализа данных для решения профессиональных задач посредством применения современных инструментальных и программных средств	**Знать:** – фундаментальные разделы математики; – методы системного анализа; **Уметь:** – использовать законы естественно-научных дисциплин в профессиональной деятельности и применять математический аппарат, методы оптимизации, теории вероятностей, математической статистики, системного анализа для принятия решений в области решения профессиональных задач; – применять методы анализа данных; – применять инструментальные и программные средства для анализа данных; **Владеть** навыками анализа данных для решения профессиональных задач с применением современных технологий.

Форма обучения: очная.

IV. Формы контроля

Контроль за освоением дисциплины осуществляется в каждом дисциплинарном разделе отдельно.

Рубежный контроль: тестирование и контрольная работа по отдельным разделам дисциплины.

Итоговая аттестация в 3 семестре – зачет.

Результаты текущего контроля и итоговой аттестации формируют рейтинговую оценку работы обучающегося. Распределение баллов по отдельным видам работ в процессе освоения дисциплины «разработка мобильных приложений» осуществляется в соответствии с Приложением 1.

V. Объём дисциплины и виды учебной работы

Объем курса – 72 часа, 2 зачетные единицы, в том числе 30 часа – аудиторная нагрузка, из которых 6 часов – лекции, 24 часов – семинары, 42 часов – самостоятельная работа студентов. Изучается на 2 курсе (3 семестр), итоговая форма отчетности – зачет.

Вид учебной работы	Всего часов
Контактные занятия (всего)	30
В том числе:	-
Лекции	6
Практические занятия (ПЗ)	-
Семинары (С)	24
Лабораторные работы (ЛР)	-
Самостоятельная работа (всего)	42
В том числе:	-
Домашние задания	12
Реферат	8
Подготовка к тестированию	8
Подготовка к опросу	5
Подготовка к контрольной работе	5
Вид промежуточной аттестации Зачет	4
Общая трудоемкость (часы) Зачетные единицы	72 2

VI. Структура и содержание дисциплины

п/п	Раздел	Содержание (темы)
1	**Основные понятия и определения**	Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; классификация сетевых атак; цели и задачи обеспечения безопасности: доступность, целостность, конфиденциальность, ответственность, гарантирование; модели сетевой безопасности и безопасности информационной системы.
2	**Алгоритмы симметричного шифрования**	Основные понятия алгоритмов симметричного шифрования, ключ шифрования, plaintext, ciphertext;

		стойкость алгоритма, типы операций, сеть Фейштеля; алгоритмы DES и тройной DES. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147, режимы их выполнения; способы создания псевдослучайных чисел. Новый стандарт алгоритма симметричного шифрования – AES; критерии выбора алгоритма и сравнительная характеристика пяти финалистов; понятие резерва безопасности. Характеристики алгоритмов, особенности программной реализации, возможность их реализации в окружениях с ограничениями пространства, возможность вычисления на лету подключей. Алгоритм Rijndael; математические понятия, лежащие в основе алгоритма Rijndael; структура раунда алгоритма Rijndael.
3	**Криптография с открытым ключом.**	Основные понятия криптографии с открытым ключом, способы ее использования: шифрование, создание и проверка цифровой подписи, обмен ключа. Алгоритмы RSA и Диффи-Хеллмана.
4	**Хэш-функции и аутентификация сообщений.**	Основные понятия обеспечения целостности сообщений с помощью MAC и хэш-функций; простые хэш-функции. Сильные хэш-функции MD5, SHA-1, SHA-2, SHA-3 и ГОСТ 3411; обеспечение целостности сообщений и вычисление MAC с помощью алгоритмов симметричного шифрования, хэш-функций и стандарта HMAC.
5	**Цифровая подпись.**	Требования к цифровым подписям, стандарты цифровой подписи ГОСТ 3410 и DSS.
6	**Алгоритмы обмена ключей и протоколы аутентификации.**	Понятия инфраструктуры открытого ключа: сертификат открытого ключа, сертификационный центр, конечный участник, регистрационный центр, CRL, политика сертификата, регламент сертификационной практики, проверяющая сторона, репозиторий; архитектура PKI. Профиль сертификата X.509 v3 и профиль CRL v2; сертификационный путь; основные поля сертификата и расширения сертификата; критичные и некритичные расширения; стандартные расширения. Профиль CRL v2 и расширения CRL, области CRL, полный CRL, дельта CRL; Алгоритм проверки действительности сертификационного пути. Протоколы PKI управления сертификатом. On-line протокол определения статуса сертификата; политика сертификата и регламент сертификационной практики. Сервис директории LDAP, сравнение LDAP с реляционными базами данных; информационная модель LDAP, модель именования LDAP, понятие дерева директории, DN, схемы, записи, атрибута записи, класса объекта. Основные свойства протокола LDAP. Abstract Syntax Notation One (ASN.1); простые и структурные типы; идентификатора объекта.
7	**Протокол TLS/SSL.**	Протокол Записи и протокол Рукопожатия, понятие "состояние соединения". Полное и сокращенное Рукопожатие. Выработка общего секрета и создание из него ключевого материала с помощью псевдослучайной функции (PRF). Расширения, используемые для добавления функциональностей в протокол TLS.
8	**Семейство протоколов IPSec.**	Возможные способы реализации IPSec. Степень

		детализации управления трафиком. Протоколы ESP и AH. Политика безопасности. Способы аутентификации участников и распределение ключей.

Разделы дисциплин и виды занятий (ак. часы)

п/п	Наименование раздела дисциплины	Лекция	Практические занятия	Лабораторные занятия	Семинар	СРС	Форма текущего контроля
1	Основные понятия и определения	1	-	-	2	6	Опрос
2	Алгоритмы симметричного шифрования	1	-	-	2	4	Тест Домашнее задание
3	Криптография с открытым ключом.	1	-	-	4	4	Домашнее задание
4	Хэш-функции и аутентификация сообщений.	1	-	-	2	8	Домашнее задание КР
5	Цифровая подпись.	1	-	-	2	4	Домашнее задание
6	Алгоритмы обмена ключей и протоколы аутентификации.	1			4	4	Домашнее задание
7	Протокол TLS/SSL.	-			4	4	Домашнее задание
8	Семейство протоколов IPSec.	-			4	4	Домашнее задание
	Промежуточная аттестация (зачет)		-	-		4	
	Итого	6	-	-	24	42	

VII. Образовательные технологии

В процессе освоения дисциплины «Разработка программного обеспечения» 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 рефератов;
– групповые дискуссии и проекты;
– обсуждение результатов работы студенческих исследовательских групп.

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

Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

1. Лапонина О.Р. Курс лекций. Учебное пособие «Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия» под редакцией проф. Сухомлина В.А. 2-е издание, исправленное, изд. ООО «ИНТУИТ.ру» Интернет-Университет Информационных Технологий, 2007г. ISBN 978-5-9556-0102-1 (ИНТУИТ.РУ), ISBN 978-5-94774-650-1 (БИНОМ.ЛЗ), 531с. (33,5 усл. печ. л.), тираж 2000 экз. Рекомендовано учебно-методическим объединением в области прикладной информатики для студентов высших учебных заведений, обучающихся по специальности 510200 «Прикладная математика и информатика».

2. Лапонина О.Р. «Основы сетевой безопасности. Ч.2 Технологии туннелирования» », под редакцией проф. В.А. Сухомлина, изд. Национальный Открытый Университет «ИНТУИТ», 2014г., ISBN 978-5-9556-0163-2, 474 с. (30 усл. печ. л.), тираж 1500 экз. Допущено УМО по классическому университетскому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению ВПО 010400 «Прикладная математика и информатика» и 010300 «Фундаментальная информатика и информационные технологии».

б) Дополнительная литература:

3. James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback « Report on the Development of the Advanced Encryption Standard (AES)». Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Technology Administration U.S. Department of Commerce. 2000г. 116с.
4. Государственный Стандарт Российской Федерации «ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма» 1994г.
5. Государственный Стандарт Российской Федерации «ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Функция хэширования» 1994г.
6. RFC 2251 «Lightweight Directory Access Protocol (v3)», 1997г. 50с.

7. RFC 2252 «Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions», 1997г. 32с.
8. RFC 2253 «The String Representation of LDAP Search Filters», 1997г. 8с.
9. RFC 2256 «A Summary of the X.500(96) User Schema for use with LDAPv3», 1997г. 20с.
10. RFC 2587 «Internet X.509 Public Key Infrastructure LDAPv2 Schema», 1999г. 8с.
11. RFC 3383 «Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)», 2002г. 23с.
12. RFC 2246 «The TLS Protocol Version 1.0», 1999г. 80с.
13. RFC 3546 «Transport Layer Security (TLS) Extensions», 2003г. 29с.
14. RFC 3280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», 2002г. 129с.
15. RFC 3281 «An Internet Attribute Certificate Profile for Authorization», 2002г. 40с.
16. RFC 2401 «Security Architecture for the Internet Protocol», 1998г. 66с.
17. RFC 2408 «Internet Security Association and Key Management Protocol (ISAKMP)», 1998г. 86с.
18. RFC 2409 «The Internet Key Exchange (IKE)», 1998г. 41с.
19. RFC 2412 «The OAKLEY Key Determination Protocol», 1998г. 55с.
20. RFC 3383 «Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)», 2002г. 23с.
21. RFC 2993 «Architectural Implications of NAT», 2000г. 29с.
22. RFC 2663 «IP Network Address Translator (NAT) Terminology and Considerations», 1999г. 30с.
23. RFC 3022 «Traditional IP Network Address Translator (Traditional NAT)», 2001г. 16с.
24. RFC 3069 «VLAN Aggregation for Efficient IP Address Allocation», 2001г. 7с.
25. RFC 5389 «Session Traversal Utilities for NAT (STUN)», 2008г. 51с.
26. National Institute of Standards and Technology U.S. Department of Commerce «Intrusion Detection Systems», Special Publication 800-31, 2004 г. 51 с.
27. National Institute of Standards and Technology U.S. Department of Commerce «Guide to Intrusion Detection and Prevention Systems (IDPS)», Special Publication 800-94, 2007г. 127с.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и информационных справочных систем

Перечень профессиональных баз данных и информационных справочных систем

1. ЭБС «Юрайт» [раздел «ВАША ПОДПИСКА: учебники и учебные пособия издательства «Юрайт»]: сайт. – URL: https://www.biblio-online.ru/catalog/
2. ЭБС издательства «Лань» [учебные, научные издания, первоисточники, художественные произведения различных издательств; журналы] : сайт. – URL: http://e.lanbook.com
3. https://www.econ.msu.ru/elibrary – электронная библиотека Экономического факультета МГУ
4. https://www.nbmgu.ru – Научная библиотека МГУ

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. https://ietf.org

Рекомендуемые обучающие, справочно-информационные, контролирующие и прочие компьютерные программы, используемые при изучении дисциплины

№ п/п	Название рекомендуемых по разделам и темам программы технических и компьютерных средств обучения	Номера тем
1.	MS PowerPoint	1-6
2.	MS Excel	2-4

Методические указания для обучающихся по освоению дисциплины

В процессе изучения курса обучающиеся обязаны соблюдать дисциплину, вовремя приходить на занятия, делать домашние задания, осуществлять подготовку к семинарам и контрольным работам, проявлять активность на занятиях.

При этом важное значение имеет самостоятельная работа, которая направлена на формирование у учащегося умений и навыков правильного оформления конспекта и работы с ним, работы с литературой и электронными источниками информации, её анализа, синтеза и обобщения. Для проведения самостоятельной работы обучающимся предоставляется список учебно-методической литературы.

Материально-техническое обеспечение дисциплины

Для проведения образовательного процесса необходима аудитория, оборудованная компьютером и проектором, необходимыми для демонстрации презентаций. Обязательное программное обеспечение – MS Office.

IX.ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Темы курсовых работ

Курсовая работа по дисциплине « Проектирование баз данных» не предусмотрена.

Домашние работы

Пример задания № 1. Требуется реализовать на C# программу, визуализирующую работу светофора. Светофор переключает сигналы с некоторыми интервалами: красный горит K секунд, желтый горит M секунд, зеленый горит N секунд. Сигналы переключаются в указанной последовательности до тех пор, пока программа не будет закрыта. На форме располагаются три элемента управления TrackBar по одному напротив каждого сигнала светофора, задающие параметры K, L и M.

Пример задания № 2. Требуется разработать программу, позволяющую строить задаваемую пользователем ломаную линию и производить ряд настроек её отображения. Главная форма должна отображать ломаную, вершины которой пользователь указывает, щёлкая в нужном месте левой кнопкой «мыши». Щелчки «мышью» достраивают ломаную, добавляя к ней отрезок, соединяющий точки последнего и предыдущего щелков. Кнопка «Параметры», расположенная на главном окне, должна открывать дополнительное окно для задания следующих параметров отображения ломаной: цвет ломанной, цвет фона, толщина линии.

Вопросы для текущего контроля студентов

В качестве оценочных средств для промежуточного контроля выступают результаты сдачи заданий текущей аттестации

1.	1. **Политика безопасности – это (выберите самое точное определение, *один ответ*)**	
	1. Совокупность административных мер, которые определяют порядок прохода в компьютерные классы.	
	2. Множество критериев для предоставления сервисов безопасности.	
	3. Совокупность как административных мер, так и множества критериев для предоставления сервисов безопасности.	+
	4. Межсетевые экраны, используемые в организации.	
	2. **При разработки политики безопасности главное, что должен определить собственник информационных активов (*один ответ*)**	
	1. Информационные ценности, безопасность которых следует обеспечивать.	+
	2. Атаки, которые возможны на информационные ценности.	
	3. Множество файлов, доступ к которым должен быть запрещен.	
	4. Множество сервисов, которые не должны быть доступны посторонним.	
	3. **Какие понятия не определяют полностью политику безопасности**	
	1. Множество коммутаторов и межсетевых экранов, используемых в организации.	+
	2. Совокупность как административных мер, так и множества критериев для предоставления сервисов безопасности.	
	3. Административные меры, определяющие порядок доступа в помещение.	+
	4. Административные меры, определяющие порядок доступа к рабочим станциям и серверам.	+
2.	1. **Что из перечисленного всегда является уязвимостью**	
	1. Слабое место в системе, с использованием которого может быть осуществлена атака.	+
	2. Ошибка в программном обеспечении.	
	3. Отсутствие политики безопасности.	
	4. Ошибка в настройках межсетевого экрана.	
	2. **Что из перечисленного может не являться уязвимостью**	
	1. Слабое место в системе, с использованием которого может быть осуществлена атака.	
	2. Ошибка в программном обеспечении.	+
	3. Ошибка в настройках межсетевого экрана.	+
	4. Ошибка в настройках маршрутизации.	+
	3. **Что понимается под атакой на информационную систему**	
	1. Любое действие, нарушающее безопасность информационной системы.	+

	2. Действие или последовательность связанных между собой действий, использующих уязвимости данной информационной системы и приводящих к нарушению политики безопасности.	+
	3. Использование ошибки в программном обеспечении.	
	4. Исключительно несанкционированный доступ в систему.	
3.	1. **Механизм безопасности – это (выберите самое точное определение, *один ответ*)**	
	1. Программное и/или аппаратное средство, которое определяет и/или предотвращает атаку.	+
	2. Настройки межсетевого экрана.	
	3. Настройки программного обеспечения.	
	4. Аппаратура, которая предотвращает несанкционированный доступ к файлам и программам.	
	2. **Сервис безопасности – это**	
	1. Сервис, который обеспечивает задаваемую политикой безопасность информационных систем и/или передаваемых данных.	+
	2. Сервис, который определяет осуществление атаки.	+
	3. Сервис, который предотвращает несанкционированный доступ к файлам и программам.	+
	4. Сервис, который обеспечивает взаимодействие с вышестоящей организацией.	
	3. Что не относится к сервисам безопасности	
	1. Используемые математические алгоритмы.	+
	2. Предотвращение несанкционированного доступа.	
	3. Обнаружение и документирование проникновения.	
	4. Выполнение аутентификации сервера.	
4.	1. **Причины, по которым необходимо создавать «оборону в глубину»**	
	1. Ни один из сервисов безопасности не может гарантировать 100%-ную защиту.	+
	2. Сбой единственного используемого сервиса безопасности не должен означать, что нарушитель получает полный доступ в систему.	+
	3. Межсетевой экран не может быть конечной точкой VPN.	
	4. Межсетевой экран не может выполнять аутентификацию пользователей.	
	2. **Что понимают под «обороной в глубину»**	
	1. Создание такой информационной инфраструктуры, в которой для минимизации отказов и проникновений используются несколько взаимосвязанных между собой технологий.	+
	2. Создание такой информационной инфраструктуры, в которой используется несколько межсетевых экранов.	

	3. Создание такой сетевой топологии, в которой используются межсетевые экраны нескольких производителей.	
	4. Создание такой сетевой топологии, в которой используются межсетевые экраны одного производителя.	
	3. **Что не относится к понятию «оборона в глубину»**	
	1. Использование нескольких взаимосвязанных между собой технологий.	
	2. Использование нескольких коммутаторов.	+
	3. Использование нескольких межсетевых экранов.	+
	4. Использование аппаратных средств разных производителей.	+
5.	1. **Под безопасностью информационной системы понимается**	
	1. Защита от неавторизованного доступа или модификации информации во время хранения, обработки или пересылки.	+
	2. Защита от отказа в обслуживании законных пользователей.	+
	3. Меры, необходимые для определения, документирования и учета угроз.	+
	4. Отсутствие выхода в интернет.	
	2. **Риск - это**	
	1. Вероятность того, что конкретная атака будет осуществлена с использованием конкретной уязвимости.	+
	2. Невозможность ликвидировать все уязвимости в информационной системе.	
	3. Невозможность исправить все ошибки в программном обеспечении.	
	4. Вероятность того, что в системе остались неизвестные уязвимости.	
	3. **Основные классы атак на передаваемые по сети данные**	
	1. Активная и пассивная.	+
	2. Видимая и невидимая.	
	3. Удаленная и локальная.	
	4. Внешняя и внутренняя.	
6.	1. **Под reply-атакой понимается**	
	1. Модификация передаваемого сообщения.	
	2. Повторное использование нарушителем перехваченного ранее сообщения.	+
	3. Невозможность получения сервиса законным пользователем.	
	4. Просмотр передаваемого сообщения.	
	2. **Повторное использование перехваченного ранее сообщения называется**	
	1. DoS-атакой.	

	2. Replay-атакой.	+
	3. DDoS-атакой.	
	4. Атакой «man-in-the-middle».	
	3. **Что не относится к replay-атаке**	
	1. Повторное использование нарушителем перехваченного ранее сообщения.	
	2. Изменение передаваемых данных.	+
	3. Выполнение незаконного проникновения в систему.	+
	4. Просмотр передаваемых данных.	+
7.	1. **Под DoS-атакой понимается**	
	1. Модификация передаваемого сообщения.	
	2. Повторное использование нарушителем перехваченного ранее сообщения.	
	3. Невозможность доступа в систему законным пользователем.	
	4. Невозможность получения сервиса законным пользователем.	+
	2. **Невозможность получения сервиса законным пользователем называется**	
	1. DoS-атакой.	+
	2. Replay-атакой.	
	3. Пассивной атакой.	
	4. Атакой «man-in-the-middle».	
	3. **Что не относится к DoS-атаке**	
	1. Выполнение незаконного проникновения в систему.	+
	2. Определение топологии сети.	+
	3. Попытка исчерпать какие-либо ресурсы на целевой системе.	
	4. Попытка монополизировать сетевое соединение.	
8.	1. **Атака «man in the middle» является**	
	1. Пассивной.	
	2. Активной.	+
	3. Видимой.	
	4. Может быть как активной, так и пассивной.	
	2. **Что не относится к атаке «man in the middle»**	
	1. Выполнение незаконного проникновения в систему.	+

	2. Просмотр передаваемых данных.	+
	3. Изменение передаваемых данных.	
	4. Исчерпание ресурсов на целевой системе.	+
	3. **Модификация передаваемого сообщения называется**	
	1. DoS-атакой.	
	2. Replay-атакой.	
	3. Пассивной атакой.	
	4. Атакой «man in the middle».	+
9.	1. **Атака называется пассивной, если**	
	1. Оппонент не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения.	+
	2. Оппонент не анализирует перехваченные сообщения.	
	3. Оппонент не предполагает проникновение в систему.	
	4. Оппонент не использует никаких инструментальных средств для выполнения атаки.	
	2. **Что не относится к пассивной атаке**	
	1. Изменение передаваемых данных.	+
	2. Просмотр передаваемых данных.	
	3. Выполнение незаконного проникновения в систему.	+
	4. Изучение топологии сети.	
	3. **Активной называется такая атака, при которой**	
	1. Оппонент имеет возможность модифицировать передаваемые сообщения.	+
	2. Оппонент использует какое-либо инструментальное средство.	
	3. Оппонент имеет возможность вставлять свои сообщения.	+
	4. Оппонент анализирует перехваченные сообщения.	
10.	1. **Атака сканирования является разновидностью**	
	1. Пассивной атаки.	+
	2. Активной атаки.	
	3. Законной атаки.	
	4. Невидимой атаки.	
	2. **Атаки сканирования могут определять**	

	1. Топологию целевой сети.	+
	2. Типы сетевого трафика, пропускаемые межсетевым экраном.	+
	3. Операционные системы, которые выполняются на хостах.	+
	4. ПО сервера, которое выполняется на хостах.	+
	5. Номера версий для всего обнаруженного ПО.	+
	3. **Сканирование сети**	
	1. Всегда является атакой.	
	2. Не является атакой.	
	3. Является ли атакой – определяется политикой безопасности.	+
	4. Является ли атакой – определяется настройками межсетевого экрана.	
11.	1. **Атаки сканирования**	
	1. Могут выполняться теми же инструментальными средствами, которые используются законными поисковыми системами в интернете.	+
	2. Должны выполняться специальными инструментальными средствами.	
	3. Могут выполняться теми же инструментальными средствами, которые используют межсетевые экраны.	
	4. Могут выполняться теми же инструментальными средствами, которые используют маршрутизаторы.	
	2. **Что не относится к атаке сканирования**	
	1. Выполнение незаконного проникновения в систему.	+
	2. Определение версий установленного ПО.	
	3. Определение номеров открытых портов.	
	4. Определение топологии сети.	
	3. **Что не относится к активной атаке**	
	1. Изменение передаваемых данных.	
	2. Просмотр передаваемых данных.	+
	3. Изучение топологии сети.	+
	4. Определение версий установленного ПО.	+
12.	1. **Разновидности DoS-атак**	
	1. DoS-атаки шквальной эксплуатации.	+
	2. DoS-атаки наводнения.	+
	3. DoS-атаки, использующие ресурсы заранее взломанных компьютеров.	

	4. DoS-атаки проникновения.	
	2. **DoS-атаки шквальной эксплуатации**	
	1. Приводят к исчерпанию ресурсов на целевой системе.	+
	2. Приводят к исчерпанию ресурсов атакующего.	
	1. Приводят к запуску всех программ, установленных на целевой системе.	
	2. Приводят к открытию всех портов на целевой системе.	
	3. **При DoS-атаках наводнения**	
	1. Атакующий попытается монополизировать сетевое соединение с целевой системой.	+
	2. Атакующий попытается выполнить несанкционированный доступ в систему.	
	3. Атакующий попытается исчерпать какие-либо ресурсы в целевой системе.	
	4. Атакующий пытается получить несколько вариантов доступа в систему.	
13.	1. **Конфиденциальность – это**	
	1. Невозможность несанкционированного изменения данных.	
	2. Невозможность несанкционированного просмотра данных.	+
	3. Невозможность несанкционированного выполнения программ.	
	4. Невозможность несанкционированного доступа к данным.	
	2. **Сервис, который обеспечивает невозможность несанкционированного просмотра данных, называется**	
	1. Аутентификацией.	
	2. Целостностью.	
	3. Недоступностью.	
	4. Конфиденциальностью.	+
	3. **Что из перечисленного относится к сервисам безопасности**	
	1. Алгоритмы асимметричного шифрования.	
	2. Обеспечение целостности.	+
	3. Обеспечение конфиденциальности.	+
	4. Алгоритмы симметричного шифрования.	
14.	1. **Целостность – это**	
	1. Невозможность несанкционированного просмотра информации.	
	2. Невозможность несанкционированного изменения информации.	+

	3. Невозможность несанкционированного выполнения программ.	
	4. Невозможность несанкционированного доступа к информации.	
	2. **Сервис, который обеспечивает невозможность несанкционированного изменения данных, называется**	
	1. Аутентификацией.	
	2. Целостностью.	+
	3. Доступностью.	
	4. Конфиденциальностью.	
	3. **Доступность - это**	
	1. Гарантирование того, что авторизованные пользователи могут иметь доступ к информационным ресурсам, и при этом обеспечивается требуемая производительность.	+
	2. Гарантирование того, что все пользователи могут иметь доступ к информационным ресурсам.	
	3. Гарантирование того, что информационные ресурсы доступны 24 часа в сутки, 7 дней в неделю.	
	4. Гарантирование того, что информационные ресурсы могут быть изменены любым пользователем.	
15.	1. **Аутентификация – это**	
	1. Невозможность несанкционированного доступа к данным.	
	2. Подтверждение того, что информация получена из законного источника и получателем является тот, кто нужно.	+
	3. Невозможность несанкционированного просмотра информации.	
	4. Невозможность несанкционированной модификации информации.	
	2. **Сервис, который гарантирует, что информация получена из законного источника и получателем является тот, кто нужно, называется**	
	1. Аутентификацией.	+
	2. Целостностью.	
	3. Конфиденциальностью.	
	1. Доступностью.	
	3. **Авторизация - это**	
	1. Сервис, который определяет права и разрешения, предоставляемые индивидууму (или процессу) и обеспечивает возможность доступа к ресурсу.	+
	2. Подтверждение того, что информация получена из законного источника и получателем является тот, кто нужно.	
	3. Невозможность несанкционированной модификации информации.	

	4. Невозможность несанкционированного просмотра информации.	
16.	1. **Идентификация – это**	
	1. Сервис, с помощью которого указываются уникальные атрибуты пользователей, позволяющие отличать пользователей друг от друга.	+
	2. Сервис, с помощью которого пользователь указывает свою фамилию администратору.	
	3. Сервис, с помощью которого прикладной сервер передает свой IP-адрес.	
	4. Сервис, с помощь которого можно получить подтверждение, что информация получена из законного источника и получателем является тот, кто нужно.	
	2. **Для гарантирования выполнения сервисов безопасности необходимо**	
	1. Разработать политику безопасности.	+
	2. Рассмотреть существующие нормативные требования и акты.	+
	3. Обеспечить обучение сотрудников, ответственных за ИБ.	+
	4. Обеспечить отсутствие посторонних лиц в организации.	
	3. **Отчетность включает**	
	1. Создание и аудит системных логов.	+
	2. Мониторинг систем и сетевого трафика.	+
	3. Обнаружение проникновений.	+
	4. Фильтрование нежелательного трафика.	
17.	1. **Анализ рисков включает**	
	1. Идентификацию и приоритезацию информационных активов.	+
	2. Идентификацию и категоризацию угроз этим активам.	+
	3. Приоритезацию рисков.	+
	4. Идентификацию посторонних лиц в организации.	
	2. **Возможные стратегии управления рисками**	
	1. Принять риск.	+
	2. Уменьшить риск.	+
	3. Передать риск.	+
	4. Избежать риск.	+
	3. **В случае принятия риска необходимо**	
	1. Иметь полное представление о потенциальных угрозах и уязвимостях для информационных активов.	+
	2. Не подключать сеть организации к интернету.	

	3. Закрыть все порты в системе.	
	4. Не хранить в системе важные информационные ресурсы.	
18.	1. **Под угрозой понимается**	
	1. Любое событие, которое может иметь нежелательные последствия для организации.	+
	2. Присутствие посторонних лиц в организации.	
	3. Наличие большого числа открытых портов в системе.	
	4. Наличие большого количества ПО, установленного на каждой системе.	
	2. **Примеры угроз**	
	1. Возможность раскрытия, модификации, уничтожения информационных активов.	+
	2. Невозможность использования информационных активов.	+
	3. Проникновение или любое нарушение функционирования информационной системы.	+
	4. Открытый порт в системе.	
	3. **Примерами уязвимостей являются**	
	1. Наличие слабых мест в ПО.	+
	2. Наличие слабых мест в сетевой топологии.	+
	3. Наличие слабых мест, связанных с человеческим фактором.	+
	4. Наличие открытых портов в системе.	
19.	1. **Участниками аутентификационного процесса могут быть**	
	1. Пользователи.	+
	2. Маршрутизаторы.	+
	3. Межсетевые экраны.	+
	4. Пароли.	
	2. **Идентификация пользователя дает возможность вычислительной системе**	
	1. Отличать одного пользователя от другого.	+
	2. Гарантировать, что пользователь является тем, за кого он себя выдает.	
	3. Обеспечить корректное управление доступом.	
	4. Гарантировать отсутствие несанкционированного доступа.	
	3. **Термин сущность (entity) часто лучше подходит для обозначения предъявителя идентификации, чем термин пользователь, так как**	
	1. Участниками аутентификационного процесса могут быть не только	+

	пользователи, но и программы и аппаратные устройства.	
	2. Участниками аутентификационного процесса являются не пользователи, а прикладные сервера.	
	3. Участниками аутентификационного процесса являются не пользователи, а межсетевые экраны.	
	4. Участниками аутентификационного процесса являются не пользователи, а аппаратные устройства.	
20.	1. **В качестве аутентификации пользователя могут использоваться**	
	1. Пароли.	+
	2. Цифровые сертификаты.	+
	3. Биометрические параметры.	+
	4. Фамилия пользователя.	
	2. **Многофакторная аутентификация означает**	
	1. Аутентифицируемой стороне необходимо предоставить несколько параметров, чтобы установить требуемый уровень доверия.	+
	2. Аутентификация не может выполняться с помощью пароля.	
	3. Аутентификация должна выполняться третьей доверенной стороной.	
	4. Аутентификация должна выполняться с использованием смарт-карты.	
	3. **Централизованное управление идентификационными и аутентификационными данными имеет следующие преимущества**	
	1. Легкое администрирование.	+
	2. Возможность использования многофакторной аутентификации.	
	3. Возможность использования цифровых подписей.	
	4. Возможность использования третьей доверенной стороны.	
21.	1. **Управление доступом или авторизация означает**	
	1. Определение прав и разрешений пользователей по доступу к ресурсам.	+
	2. Гарантирование того, что пользователь является тем, за кого он себя выдает.	
	3. Гарантирование того, что пользователь обращается к требуемому ресурсу (серверу).	
	4. Невозможность несанкционированного просмотра и изменения данных.	
	2. **Основные компоненты управления доступом**	
	1. Субъекты.	+
	2. Объекты или ресурсы.	+
	3. Разрешения (привилегии).	+

	4. Маршрутизаторы.	
	3. **В системах управления доступом субъектом может быть**	
	1. Пользователь.	+
	2. Аппаратное устройство.	+
	3. Процесс ОС.	+
	4. Прикладная система.	+
22.	1. **В системах управления доступом объектом может быть**	
	1. Файл.	+
	2. Любой сетевой ресурс, к которому субъект хочет получить доступ.	+
	3. Аппаратное устройство.	+
	4. Прикладная система.	+
	2. **При управлении доступом на уровне файловой системы для разграничения доступа используются**	
	1. Списки управления доступом (Access Control List – ACL).	+
	2. Правила фильтрования межсетевого экрана.	
	3. БД политик безопасности.	
	4. Статические маршруты.	
	3. **При управление доступом на сетевом уровне для разграничения трафика используются**	
	1. Маршрутизаторы.	+
	2. Межсетевые экраны.	+
	3. Коммутаторы.	
	4. Веб-сервера.	
23.	1. **Гарантирование доступности предполагает**	
	1. Определение точек возможного сбоя и ликвидация этих точек.	+
	2. Определение критически важных устройств.	+
	3. Определение критически важных сервисов.	+
	4. Определение списков управления доступом.	
	2. **При управлении конфигурациями необходимо обеспечить следующее**	
	1. Регулярное обновление ПО.	+
	2. Управление изменениями.	+

	3. Оценка состояния сетевой безопасности.	+
	4. Регулярное изменение правил фильтрования.	
	3. **При возникновении инцидента, связанного с информационной безопасностью, самое главное, что необходимо иметь (один ответ)**	
	1. Эффективные способы его распознавания.	+
	2. Эффективные способы предотвращения последующих инцидентов.	
	3. Эффективные способы изменения правил фильтрования трафика.	
	4. Эффективные способы создания логов.	
24.	1. **Использование третьей доверенной стороны необходимо для**	
	1. Распределения между двумя участниками секретной информации, которая не стала бы доступна оппоненту.	+
	2. Решения споров между двумя участниками.	+
	3. Создания зашифрованных туннелей.	
	4. Изменения правил фильтрования трафика.	
	2. **Что из перечисленного относится к механизмам безопасности**	
	1. Хэш-функции.	+
	2. Целостность сообщения.	
	3. Алгоритмы симметричного шифрования.	+
	4. Аутентификация сообщения.	
	3. **Что из перечисленного не относится к механизмам безопасности**	
	1. Хэш-функции.	
	2. Целостность сообщения.	+
	3. Алгоритмы симметричного шифрования.	
	4. Аутентификация сообщения.	+

1. Алгоритмы симметричного шифрования

1.	1. **В алгоритмах симметричного шифрования секретным должен быть**	
	1. Ключ.	+
	2. Весь алгоритм симметричного шифрования.	
	3. Параметры выполнения алгоритма симметричного шифрования.	

	4. Отдельные элементы алгоритма симметричного шифрования (такие как S-box).	
	2. **Криптографическая система называется симметричной, потому что**	
	1. Шифруемый блок разбивается на подблоки одинаковой длины.	
	2. Для шифрования и расшифрования используются одинаковые или легко выводимые один из другого ключи.	+
	3. Алгоритм использует циклически повторяющиеся операции, называемые раундами.	
	4. Алгоритм использует подключи одинаковой длины.	
	3. **Зависимость между ключами шифрования и расшифрования в алгоритмах симметричного шифрования должна быть следующей**	
	1. Ключи шифрования и расшифрования должны в точности совпадать.	+
	2. Ключ расшифрования должен легко получаться из ключа шифрования.	+
	3. Между ключами шифрования и расшифрования не должно быть никакой зависимости.	
	4. Ключи шифрования и расшифрования связаны формулой, но из ключа шифрования должно быть вычислительно трудно найти ключ расшифрования.	
2.	1. **На вход алгоритму симметричного шифрования подается**	
	1. Ключ.	+
	2. Исходное незашифрованное сообщение.	+
	3. Параметры выполнения алгоритма.	
	4. Текущие дата и время.	
	2. **Выходом алгоритма симметричного шифрования является**	
	1. Зашифрованное сообщение.	+
	2. Ключ.	
	3. Текущие дата и время.	
	4. Параметры окружения, в котором выполнялся алгоритм.	
	3. **Алгоритм симметричного шифрования обозначается**	
	1. C = EK [P].	+
	2. Y = F (X).	

	3. X = F-1 (Y).	
	4. Y = FK (X).	
3.	1. **При использовании алгоритмов симметричного шифрования целью противника является**	
	1. Узнать ключ.	+
	2. Узнать пароль пользователя.	
	3. Узнать используемый алгоритм.	
	4. Узнать дату и время шифрования.	
	2. **При использовании алгоритмов симметричного шифрования целью противника является**	
	1. Узнать исходное сообщение.	+
	2. Узнать зашифрованное сообщение.	
	3. Узнать пароль сервера.	
	4. Узнать параметры окружения, в котором выполнялся алгоритм.	
	3. **Алгоритм симметричного шифрования называется блочным, если**	
	1. Алгоритм основан на сети Фейштеля.	
	2. Для шифрования исходный текст разбивается на блоки фиксированной длины.	+
	3. В алгоритме используются S-box.	
	4. В алгоритме используются циклически повторяющиеся операции.	
4.	1. **В алгоритмах симметричного шифрования используются только следующие операции**	
	1. Операции перестановки и сдвига.	
	2. S-box – i битов заменяются на j битов.	
	3. Любые из перечисленных выше операций, а также многие другие.	+
	4. Побитовое исключающее или (XOR)	
	2. **В алгоритмах симметричного шифрования S-box называется**	
	1. Циклический сдвиг на переменное число битов.	
	2. Табличная подстановка, при которой группа битов отображается в другую	+

	группу битов.	
	3. Переупорядочивание битов во всем блоке.	
	4. Сложение по модулю 2 (XOR) битов небольшого блока с подключом.	
	3. **Циклическое повторение операций в алгоритме симметричного шифрования называется**	
	1. Раундами.	+
	2. Блоками.	
	3. Сетью Фейштеля.	
	4. Симметричным алгоритмом.	
5.	1. **Ключ, используемый в каждом раунде алгоритма симметричного шифрования, называется**	
	1. Подключом.	+
	2. Ключом раунда.	+
	3. Ключом сессии.	
	4. Мастер-ключом.	
	2. **С увеличением количества раундов стойкость алгоритма**	
	1. Увеличивается.	+
	2. Уменьшается.	
	3. Увеличивается пропорционально увеличению количества раундов.	
	4. Не изменяется.	
	3. **Для увеличения стойкости алгоритма симметричного шифрования количество раундов следует**	
	1. Уменьшить.	
	2. Увеличить.	+
	3. Удвоить.	
	4. Переупорядочить.	
6.	1. **Платформы, на которых могут использоваться алгоритмы симметричного шифрования**	
	1. Мощные сервера.	+

	2. Пользовательские рабочие станции.	+
	3. Устройства, содержащие встроенные микроконтроллеры.	+
	4. Смартфоны.	+
	2. **Платформы, на которых могут использоваться алгоритмы симметричного шифрования**	
	1. Ноутбуки.	+
	2. Смарт-карты.	+
	3. Маршрутизаторы.	+
	4. Настраиваемые коммутаторы.	+
	3. **Реализация алгоритма симметричного шифрования может быть**	
	1. Программной, с открытым кодом.	+
	2. Программной, с закрытым кодом.	
	3. Аппаратной.	+
	4. Программной, лицензированной уполномоченным органом.	
7.	1. **Сеть Фейштеля широко используется при разработке алгоритмов симметричного шифрования, потому что**	
	1. Увеличение количества раундов сети Фейштеля приводит к увеличению стойкости алгоритма шифрования.	+
	2. Для обратимости сети Фейштеля не требуется обратимость образующей функции F.	+
	3. Сеть Фейштеля достаточно компактна и проста в реализации.	+
	4. Других способов реализации алгоритмов симметричного шифрования не существует.	
	2. **Сеть Фейштеля имеет следующую структуру**	
	1. Входной блок делится на несколько равной длины подблоков, называемых ветвями.	+
	2. Каждая ветвь обрабатывается независимо от другой.	+
	3. Каждая ветвь обрабатывается по одному и тому же алгоритму.	
	4. После обработки каждой ветви осуществляется циклический сдвиг всех ветвей влево.	+
	3. **Под плоским пространством ключей понимают**	

	1. Возможность использования любой последовательности битов в качестве ключа.	+
	2. Возможность вычислять ключ из двух параметров X и Y.	
	3. Возможность получать ключ из области внешней памяти.	
	4. Возможность вычислять ключ без использования параметров, связанных со временем.	
8.	1. **Криптоанализ – это процесс, при котором**	
	1. Зная зашифрованное сообщение, пытаются узнать незашифрованное сообщение.	+
	2. Зная одну или несколько пар (незашифрованное сообщение, зашифрованное сообщение), пытаются узнать ключ.	+
	3. Изменяют передаваемое зашифрованное сообщение.	
	4. Пытаются узнать используемый алгоритм шифрования.	
	2. **Криптографическая система считается вычислительно безопасной, если**	
	1. Невозможно расшифровать сообщение без знания ключа шифрования.	
	2. Цена расшифровки сообщения больше цены самого сообщения.	+
	3. Время, необходимое для расшифровки сообщения, больше времени жизни сообщения.	+
	4. Невозможно определить ключ шифрования.	
	3. **Алгоритм симметричного шифрования может использоваться**	
	1. Для шифрования данных.	+
	2. Для создания случайных чисел.	+
	3. В качестве алгоритма хэширования.	+
	4. Для создания цифровой подписи.	
9.	1. **Основные критерии, используемые при разработки алгоритмов симметричного шифрования**	
	1. Алгоритм должен иметь размер блока 64 или 128 бит.	+
	2. Алгоритм должен иметь разные ключи для шифрования и расшифрования.	
	3. Использовать простые операции, которые эффективны на микропроцессорах.	+
	4. Должна быть возможность реализации алгоритма на 8-битном процессоре с минимальными требованиями к памяти.	+

	2. **Основные критерии, используемые при разработки алгоритмов симметричного шифрования**	
	1. По возможности не иметь слабых ключей.	+
	2. Алгоритм должен иметь масштабируемый ключ до 256 бит.	+
	3. Ключ расшифрования не должен вычисляться из ключа шифрования.	
	4. Алгоритм расшифрования должен совпадать с алгоритмом шифрования.	
	3. **Выберите правильное утверждение**	
	1. В основе алгоритма DES лежит сеть Фейштеля.	+
	2. В алгоритме DES используются S-boxes.	+
	3. В алгоритме DES используется умножение по модулю 216 + 1.	
	4. Алгоритм DES не является итерационным.	
10.	1. **Длина ключа в алгоритме DES равна**	
	1. 56 бит.	+
	2. 56 байт.	
	3. 128 бит.	
	4. 256 бит.	
	2. **Количество раундов в алгоритме DES равно**	
	1. 16.	+
	2. 24.	
	3. 32.	
	4. 256.	
	3. **Длина блока в алгоритме DES равна**	
	1. 64 бита.	+
	2. 128 битов.	
	3. 64 байта.	
	4. 128 байтов.	

11.	1. **При расшифровании DES подключи используются**	
	1. В том же порядке, что и при шифровании.	
	2. В обратном порядке относительно их использования при шифровании.	+
	3. В произвольном порядке.	
	4. Подключи расшифрования не зависят от подключей шифрования.	
	2. **Двойной DES не используется, потому что**	
	1. Недостаточна длина ключа.	
	2. Существует атака «встреча посередине», которая позволяет снизить стойкость алгоритма до стойкости простого DES.	+
	3. Слишком сильно увеличивается сложность вычислений.	
	4. Длина ключа становится слишком большой.	
	3. **Причина использования двух, а не трех ключей в тройном DES состоит в том, что**	
	1. При использовании двух ключей отсутствует атака «встреча посередине», при использовании трех ключей существует атака «встреча посередине».	
	2. Стойкость алгоритма не повышается при использовании трех ключей вместо двух.	
	3. При использовании трех ключей общая длина ключа равна 168 битам, что может потребовать существенно больших вычислений при его распределении.	+
	4. При использовании трех ключей существенно снижается скорость шифрования.	
12.	1. **В алгоритме ГОСТ 28147**	
	1. Размер S-box постоянный.	+
	2. Размер S-box зависит от ключа.	
	3. Не используются S-box.	
	4. Размер S-box зависит от номера раунда.	
	2. **Размер S-box в алгоритме ГОСТ 28147 равен**	
	1. 4 x 4 битов.	+
	2. 6 x 4 битов.	
	3. 4 x 4 байтов.	

	4. 8 x 8 битов.	
	3. **Длина ключа в алгоритме ГОСТ 28147 равна**	
	1. 56 битов.	
	2. 256 битов.	+
	3. 56 байтов.	
	4. 256 байтов.	
13.	1. **Последовательность случайных чисел должна быть**	
	1. Монотонно возрастающей.	
	2. Непредсказуемой.	+
	3. Иметь равномерное распределение.	+
	4. Монотонно убывающей.	
	2. **Случайные числа используются в сетевой безопасности**	
	1. В схемах взаимной аутентификации.	+
	2. В качестве ключа в алгоритмах симметричного шифрования.	+
	3. Для определения последовательности передаваемых сообщений в протоколах.	
	4. Для определения последовательности операций в алгоритме симметричного шифрования.	
	3. **Свойство случайности в последовательности чисел означает**	
	1. Равномерное распределение.	+
	2. Непредсказуемость.	+
	3. Равномерное возрастание.	
	4. Использование аппаратных генераторов.	
14.	1. **В качестве генератора псевдослучайных чисел может использоваться**	
	1. Алгоритм симметричного шифрования.	+
	2. Любой математический алгоритм.	
	3. Математическая функция, не имеющая обратной функции.	

	4. Математическая функция, имеющая обратную функцию.	
	2. **В генераторе псевдослучайных чисел ANSI X9.17 используется алгоритм**	
	1. DES.	
	2. Тройной DES с двумя ключами.	+
	3. Тройной DES с тремя ключами.	
	4. AES.	
	3. **Алгоритм Rijndael характеризуется следующими свойствами**	
	1. Имеет длину блока 128 бит.	+
	2. Основан на сети Фейштеля.	
	3. Использует S-box.	+
	4. Количество слоев в раунде является параметром алгоритма и может варьироваться.	
15.	1. **Различные режимы шифрования предназначены для того, чтобы**	
	1. Обеспечить возможность обрабатывать сообщения, длина которых больше длины блока шифрования.	+
	2. Обеспечить возможность обрабатывать сообщения порциями, меньшими, чем длина блока шифрования.	+
	3. Увеличить стойкость алгоритма.	
	4. Использовать ключи шифрования разной длины.	
	2. **Режим CBC в алгоритмах симметричного шифрования используется для того, чтобы**	
	1. Одинаковые незашифрованные блоки преобразовывались в различные зашифрованные блоки.	+
	2. Не было необходимости разбивать сообщение на целое число блоков достаточно большой длины.	
	3. Увеличить скорость шифрования.	
	4. Различные незашифрованные блоки преобразовывались в одинаковые зашифрованные блоки.	
	3. **Дополнительный параметр, называемый инициализационным вектором (IV), определен в режиме**	
	1. ECB.	

	2. CBC.	+
	3. CFB.	
	4. OFB.	
16.	1. **Потокоориентированной передачи лучше всего соответствуют режимы алгоритмов симметричного шифрования**	
	1. ECB.	
	2. CBC.	
	3. CFB.	+
	4. OFB.	+
	2. **Для передачи коротких сообщений лучше всего соответствуют режимы алгоритмов симметричного шифрования**	
	1. ECB.	+
	2. CBC.	
	3. CFB.	
	4. OFB.	
	3. **Для передачи больших сообщений лучше всего соответствуют режимы алгоритмов симметричного шифрования**	
	1. ECB.	
	2. CBC.	+
	3. CFB.	
	4. OFB.	
17.	1. **Алгоритмы, входящие в число финалистов AES**	
	1. DES.	
	2. Rijndael.	+
	3. Blowfish.	
	4. Twofish.	+
	5. IDEA.	
	6. MARS.	+

	2. **Длина блока алгоритма AES должна быть не меньше**	
	1. 64 бита.	
	2. 128 битов.	+
	3. 256 битов.	
	4. 512 битов.	
	3. **Длина ключа алгоритма AES должна быть не меньше**	
	1. 56 битов.	
	2. 128 битов.	+
	3. 256 битов.	
	4. 512 битов.	
18.	1. **В качестве AES было решено выбрать**	
	1. Один алгоритм.	+
	2. Два алгоритма.	
	3. Четыре алгоритма.	
	4. Пять алгоритмов.	
	2. **Главным требованием к алгоритму была**	
	1. Низкая стоимость алгоритма.	
	2. Простота алгоритма.	
	3. Эффективность выполнения алгоритма на различных архитектурах.	
	4. Безопасность алгоритма.	+
	3. **Под окружениями с ограниченными возможностями понимают**	
	1. Устройства, обладающие небольшими объемами RAM.	+
	2. Устройства, обладающие небольшими объемами ROM.	+
	3. Устройства, имеющие небольшие физические размеры.	
	4. Устройства, не поддерживающие все протоколы интернета.	

19.	1. **Что означает гибкость алгоритма симметричного шифрования**	
	1. Возможность использовать длину ключа, отличную от той, которая должны поддерживаться обязательно.	+
	2. Возможность безопасно и эффективно реализовываться в различных типах окружений.	+
	3. Возможность использовать различные режимы выполнения алгоритма.	
	4. Возможность вести переговоры в протоколах об используемом алгоритме симметричного шифрования.	
	2. **Что означает гибкость алгоритма симметричного шифрования**	
	1. Возможность использовать длину блока, отличную от той, которая должны поддерживаться обязательно.	+
	2. Возможность использовать алгоритм в качестве поточного алгоритма шифрования, хэш-функции и предоставлять дополнительные криптографические сервисы.	+
	3. Возможность реализовать алгоритм как программно, так и аппаратно.	
	4. Возможность заменять любые компоненты алгоритма.	
	3. **Какие из алгоритмов, рассматривавшихся в качестве претендентов на AES, основаны на сети Фейштеля**	
	1. MARS.	+
	2. RC6.	+
	3. Rijndael.	
	4. Serpent.	
	5. Twofish.	+
20.	1. **Отсутствие запасного алгоритма в качестве AES обусловлено следующими причинами**	
	1. Снижается интероперабельность системы, в которой отсутствует реализация запасного алгоритма.	+
	2. Невозможно проанализировать запасной алгоритм на наличие слабых мест.	
	3. Невозможно проанализировать запасной алгоритм на наличие слабых ключей.	
	4. Снижается производительность системы, в которой есть реализация запасного алгоритма.	
	2. **Алгоритм AES должен эффективно реализовываться на следующих архитектурах**	

	1. 8-битных.	+
	2. 32-битных.	+
	3. 64-битных.	+
	4. 128-битных.	+
	3. **При принятии стандарта AES считалось, что самыми распространенными архитектурами являются**	
	1. 8-битные.	
	2. 32-битные.	+
	3. 64-битные.	
	4. 128-битные.	
21.	1. **Какому полиному соответствует шестнадцатеричное число 21**	
	1. x6 + 1	
	2. x5 + 1	+
	3. x7 + x5 + 1	
	4. x5+x4	
	2. **Какому полиному соответствует шестнадцатеричное число F8**	
	1. x6 + x5 + x4 + 1	
	2. x7 + x6 + x5 + x4 + x3 + x2 + x + 1	
	3. x7 + x6 + x5 + x4 + x3	+
	4. x8 + x7 + x6 + x5 + x4	
	3. **Какому полиному соответствует шестнадцатеричное число 3A**	
	1. x5 + x4 + x3 + x	+
	2. x6 + x5 + x3 + x	
	3. x2 + 1	
	4. x3 + x2 + x + 1	
22.	1. **В алгоритме Rijndael слой SubByte является**	

	1. Преобразованием, в котором строки состояния циклически сдвигаются на различные значения.	
	2. Побитовым XOR ключа раунда с текущим состоянием.	
	3. Нелинейной байтовой подстановкой, выполняющейся для каждого байта состояния независимо от других байтов.	+
	4. Байтовой подстановкой, подстановка для каждого следующего байта зависит от подстановки в предыдущем байте.	
	2. **S-box в алгоритме Rijndael отображает**	
	1. 1 байт в 1 байт.	+
	2. 6 битов в 4 бита.	
	3. 6 байтов в 4 байта.	
	4. 4 байта в 4 байта.	
	3. **Число раундов в алгоритме Rijndael**	
	1. Постоянное и равно 14.	
	2. Постоянное и равно 12.	
	3. Переменное и зависит от длины ключа и длины блока.	+
	4. Переменное и зависит от значения ключа.	
23.	1. **Раунд алгоритма Rijndael имеет**	
	1. 3 слоя.	
	2. 4 слоя.	+
	3. 5 слоев.	
	4. 32 слоя.	
	2. **Длина ключа в алгоритме Rijndael может быть**	
	1. 128 битов.	+
	2. 192 бита.	+
	3. 256 битов.	+
	4. 512 битов.	
	3. **Длина блока в алгоритме Rijndael может быть**	

	1. 128 битов.	+
	2. 192 бита.	+
	3. 256 битов.	+
	4. 512 битов.	
24.	1. **Выберите правильное высказывание**	
	1. В алгоритме Rijndael в слое MixColumn используется полином в GF (28).	+
	2. В алгоритме Rijndael в слое MixColumn используется полином в GF (2).	
	3. В алгоритме Rijndael в слое ByteSub используется полином в GF (28).	
	4. В алгоритме Rijndael в слое ByteSub используется полином в GF (2).	+
	2. **Выберите правильное утверждение**	
	1. В основе алгоритма Rijndael лежит традиционная сеть Фейштеля.	
	2. В основе алгоритма Rijndael не лежит сеть Фейштеля.	+
	3. В основе алгоритма Rijndael лежит сеть Фейштеля смешанного типа с 4 ветвями.	
	4. В основе алгоритма Rijndael лежит сеть Фейштеля смешанного типа с переменным количеством ветвей.	
	3. **Укажите функции, отличные от шифрования, которые могут быть выполнены алгоритмом Rijndael**	
	1. MAC (Message Authentication Code).	+
	2. Алгоритм асимметричного шифрования.	
	3. Хэш-функция.	+
	4. Генератор псевдослучайных чисел.	+

2. Криптография с открытым ключом, хэш-функции и аутентификация сообщений

1.	1. **Для создания подписи с помощью алгоритма асимметричного шифрования следует использовать**	
	1. Свой открытый ключ.	
	2. Закрытый ключ получателя.	
	3. Свой закрытый ключ.	+

	4. Открытый ключ получателя.	
	2. **Для проверки подписи с помощью алгоритма асимметричного шифрования следует использовать**	
	1. Свой открытый ключ.	
	2. Свой закрытый ключ.	
	3. Открытый ключ отправителя.	+
	4. Закрытый ключ отправителя.	
	3. **Для шифрования сообщения с помощью алгоритма асимметричного шифрования следует использовать**	
	1. Свой открытый ключ.	
	2. Открытый ключ получателя.	+
	3. Свой закрытый ключ.	
	4. Закрытый ключ получателя.	
2.	1. **Задачей факторизации числа является**	
	1. Разложение числа на простые сомножители.	+
	2. Нахождение степени, в которую следует возвести целое число для получения заданного целого числа.	
	3. Нахождение степени, в которую следует возвести простое число для получения заданного целого числа.	
	4. Нахождение произведения двух простых чисел.	
	2. **Задачей дискретного логарифмирования является**	
	1. Разложение числа на простые сомножители.	
	2. Нахождение степени, в которую следует возвести целое число для получения заданного целого числа.	+
	3. Нахождение степени, в которую следует возвести простое число для получения заданного целого числа.	
	4. Нахождение произведения двух простых чисел.	
	3. **Аутентификация сторон в алгоритме Диффи-Хеллмана необходима, потому что**	
	1. В противном случае возможен взлом задачи дискретного логарифмирования.	

	2. В противном случае возможен взлом задачи факторизации числа.	
	3. В противном случае нарушитель может заменить пересылаемые открытые ключи на свой открытый ключ.	+
	4. В противном случае нарушитель может заменить пересылаемые закрытые ключи на свой закрытый ключ.	
3.	1. **Алгоритм Диффи-Хеллмана дает возможность**	
	1. Безопасно обменяться общим секретом.	
	2. Безопасно обменяться общим секретом при условии аутентификации сторон.	+
	3. Подписать сообщение.	
	4. Зашифровать сообщение.	
	2. **Алгоритм Диффи-Хеллмана основан на невозможности решения задачи**	
	1. Дискретного логарифмирования.	+
	2. Факторизации числа.	
	3. Определения, является ли данное число простым.	
	4. Перемножения двух простых чисел.	
	3. **Аутентификация сторон в алгоритме Диффи-Хеллмана необходима, потому что**	
	1. В противном случае атакующий может перехватить передаваемые открытые ключи и заменить их своим открытым ключом.	+
	2. В противном случае атакующий может взломать дискретный логарифм.	
	3. В противном случае стороны не смогут вычислить общий секрет.	
	4. В противном случае стороны не смогут вычислить закрытые ключи друг друга.	
4.	1. **Алгоритм RSA может использоваться для**	
	1. Создания и проверки подписи.	+
	2. Шифрования.	+
	3. Обмена общим секретом.	+
	4. Авторизации.	
	2. **Алгоритм RSA основан на невозможности решения задачи**	

	1. Дискретного логарифмирования.	
	2. Факторизации числа.	+
	3. Определения, является ли данное число простым.	
	4. Нахождения произведения двух простых чисел.	
	3. **Подпись, создаваемая алгоритмом RSA, называется**	
	1. Детерминированной.	+
	2. Рандомизированной.	
	3. Необратимой.	
	4. Корректной.	
5.	1. **Хэш-функции предназначены для**	
	1. Сжатия сообщения.	
	2. Получения «отпечатков пальцев» сообщения	+
	3. Шифрования сообщения.	
	4. Кодирования сообщения.	
	2. **Выходом хэш-функции является**	
	1. Сообщение той же длины, что и входное сообщение.	
	2. Сообщение фиксированной длины.	+
	3. Сообщение меньшей длины.	
	4. Сообщение большей длины.	
	3. **Хэш-функция должна обладать следующими свойствами**	
	1. Для любого данного значения хэш-кода **h** вычислительно невозможно найти **M** такое, что **H(M) = h.**	+
	2. Хэш-функция **H** должна применяться к блоку данных фиксированной длины.	
	3. Хэш-функция **H** создает выход фиксированной длины.	+
	4. Для любого данного значения **M** вычислительно невозможно найти значение хэш-кода **h** такое, что **H(M) = h.**	
6.	1. **Хэш-функция должна обладать следующими свойствами**	

	1. Хэш-функция должна применяться к блоку данных любой длины.	+
	2. Хэш-функция должна создавать выход произвольной длины.	
	3. Для любого данного значения хэш-кода **h** вычислительно невозможно найти **M** такое, что **H(M) = h**.	+
	4. Для любого сообщения **M** вычислительно невозможно найти **h** такое, что **H(M) = h**.	
	2. **Хэш-функция должна обладать следующими свойствами**	
	1. **H(M)** относительно легко (за полиномиальное время) вычисляется для любого значения **M**.	+
	2. Для любого данного **x** вычислительно невозможно найти **y≠x**, что **H(y)=H(x)**.	+
	3. Для любого данного **x** вычислительно невозможно найти **H(x)**.	
	4. Зная **H(M)**, относительно легко (за полиномиальное время) восстановить исходное сообщение **M**.	
	3. **Свойство хэш-функции, которое гарантирует, что для любого данного значения хэш-кода h вычислительно невозможно найти M такое, что H(M)=h, позволяет**	
	1. Использовать хэш-функцию для аутентификации с помощью секретного значения.	+
	2. Использовать хэш-функцию для шифрования сообщения.	
	3. Использовать хэш-функцию для создания цифровой подписи.	
	4. Использовать хэш-функцию для обеспечения конфиденциальности сообщения.	
7.	1. **Свойство хэш-функции, которое гарантирует, что для любого сообщения M вычислительно невозможно найти M'≠M такое, что H(M)=H(M'), позволяет**	
	1. Предотвращает подделку этого сообщения, когда в качестве аутентификатора используется защищенный от изменения хэш-код.	+
	2. Предотвращает подделку этого сообщения, когда в качестве аутентификатора используется хэш-код. Дополнительной защиты хэш-кода не требуется.	
	3. Обеспечивать конфиденциальность этого сообщения.	
	4. Создавать цифровую подпись для этого сообщения.	
	2. **Требование односторонности хэш-функции состоит в следующем**	
	1. Хэш-код может быть вычислен для сообщения любой длины.	
	2. Легко создать хэш-код по данному сообщению, но вычислительно невозможно восстановить сообщение по данному хэш-коду.	+

	3. Вычислительно невозможно найти два сообщения, имеющих одинаковый хэш-код.	
	4. Невозможно найти другое сообщение с тем же самым хэш-кодом.	
	3. **Длина блоков, на которые делится сообщение в хэш-функции SHA-1, равна**	
	1. 160 битов.	
	2. 512 битов.	+
	3. 1024 битов.	
	4. 2048 битов.	
8.	1. **«Парадокс дня рождения» состоит в том, что**	
	1. Для того чтобы вероятность совпадения дней рождения у двух человек была больше 0.5, в группе должно быть всего 23 человека.	+
	2. Для того чтобы вероятность совпадения дней рождения у двух человек была больше 0.5, в группе должно быть всего 32 человека.	
	3. Для того чтобы вероятность совпадения дней рождения у двух человек была равна 1, в группе должно быть всего 23 человека.	
	4. Для того чтобы вероятность совпадения дней рождения у двух человек была равна 1, в группе должно быть всего 32 человека.	
	2. **Сколько в среднем необходимо перебрать сообщений, чтобы с вероятностью большей, чем 50%, найти сообщение с тем же самым хэш-кодом, что и данное сообщение, при условии использования сильной криптографической функции**	
	1. 2^{n-1} сообщений, где n – длина хэш-кода.	+
	2. $2^{n/2}$ сообщений, где n – длина хэш-кода.	
	3. N сообщений, где N – длина хэш-кода.	
	4. 2n сообщений, где n – длина хэш-кода.	
	3. **С точки зрения теории вероятностей «парадокс дня рождения» формулируется следующим образом**	
	1. Сколько значений Y1, …, Yk необходимо перебрать, чтобы для конкретного значения X вероятность того, что хотя бы для одного Yi выполнялось равенство H(X)=H(Y), была бы равна 1.	
	2. Сколько значений Y1, …, Yk необходимо перебрать, чтобы для конкретного значения X вероятность того, чтобы для всех Yi выполнялось равенство H(X)=H(Y), была бы больше 0,5.	
	3. Сколько значений Y1, …, Yk необходимо перебрать, чтобы для конкретного значения X вероятность того, что хотя бы для одного Yi выполнялось равенство H(X)=H(Y), была бы больше 0,5.	+

	4. Сколько значений Y1, …, Yk необходимо перебрать, чтобы для конкретного значения X вероятность того, чтобы для всех Yi выполнялось равенство H(X)=H(Y), была бы равна 1.	
9.	1. **Сколько в среднем необходимо перебрать сообщений, чтобы с вероятностью большей, чем 50%, найти два сообщения с одинаковыми хэш-кодами при условии использования сильной криптографической функции**	
	1. 2^{n-1} сообщений, где n – длина хэш-кода.	
	2. $2^{n/2}$ сообщений, где n – длина хэш-кода.	+
	3. N сообщений, где N – длина хэш-кода.	
	4. 2n сообщений, где n – длина хэш-кода.	
	2. **Если дина хэш-кода равна 128 битам, то сколько в среднем потребуется перебрать сообщений, чтобы найти сообщение с тем же самым хэш-кодом, что и данное сообщение, при условии использования сильной криптографической функции**	
	1. 2127 сообщений.	+
	2. 264 сообщений.	
	3. 2128 сообщений.	
	4. 128 сообщений.	
	3. **Если дина хэш-кода равна 128 битам, то сколько в среднем потребуется перебрать сообщений, чтобы найти два сообщения с одинаковыми хэш-кодами, при условии использования сильной криптографической функции**	
	1. 2127 сообщений.	
	2. 264 сообщений.	+
	3. 2128 сообщений.	
	4. 128 сообщений.	
10.	1. **Выберите правильное высказывание**	
	1. Каждая элементарная функция в алгоритме MD5 получает одно 32-битное слово на входе и на выходе создает три 32-битных слова.	
	2. Каждая элементарная функция в алгоритме MD5 получает три 32-битных слова на входе и на выходе создает три 32-битных слова.	
	3. Каждая элементарная функция в алгоритме MD5 получает три 32-битных слова на входе и на выходе создает одно 32-битное слово.	+
	4. Каждая элементарная функция в алгоритме MD5 получает два 32-битных слова на входе и на выходе создает одно 32-битное слово.	

	2. **Длина хэш-кода, создаваемого хэш-функцией MD5, равна**	
	1. 128 битов.	+
	2. 160 битов.	
	3. 512 битов.	
	4. 64 бита.	
	3. **Длина блоков, на которые делится сообщение, в хэш-функции MD5 равна**	
	1. 128 битов.	
	2. 512 битов.	+
	3. 1024 битов.	
	4. 64 бита.	
11.	1. **Каждый блок сообщения в хэш-функции MD5 обрабатывается**	
	1. 4 раза.	
	2. 16 раз.	
	3. 64 раза.	+
	4. 128 раз.	
	2. **Первым шагом в хэш-функции MD5 выполняется добавление битов, цель которого**	
	1. Скрыть истинную длину сообщения.	
	2. Сделать сообщение кратным 512 битам.	+
	3. Добавить случайные биты, усложняющие восстановление сообщения.	
	4. Сделать невозможным восстановление первоначального сообщения.	
	3. **Хэш-функция SHA-2 является**	
	1. Совокупностью двух функций.	
	2. Совокупностью трех функций.	+
	3. Совокупностью четырех функций.	
	4. Совокупностью 16 функций.	

12.	1. **Длина блока в хэш-функциях SHA-2 может быть**	
	1. 256 битов.	
	2. 512 битов.	+
	3. 1024 бита.	+
	4. 2048 битов.	
	2. **Длина хэш-кода в хэш-функциях SHA-2 может быть**	
	1. 256 битов.	+
	2. 384 бита.	+
	3. 512 битов.	+
	4. 1024 битов.	
	3. **Хэш-функции SHA-2 оптимизированы для архитектуры с длиной слова**	
	1. 8 битов.	
	2. 32 бита.	+
	3. 64 бита	+
	4. 128 битов.	
13.	1. **Длина блоков, на которые делится сообщение в хэш-функции ГОСТ 3411, равна**	
	1. 256 битов.	+
	2. 512 битов.	
	3. 1024 битов.	
	4. 2048 битов.	
	2. **В хэш-функции ГОСТ 3411 при вычислении промежуточного значения хэш-кода используется алгоритм симметричного шифрования ГОСТ 28147.**	
	1. Ключи для этого алгоритма являются дополнительным параметром хэш-функции ГОСТ 3411.	
	2. Ключи для этого алгоритма вычисляются по определенным формулам из хэшируемого сообщения.	+
	3. Ключи для этого алгоритма вычисляются из стартового вектора хэширования.	

	4. Ключи для этого алгоритма стандартизованы и не меняются.	
	3. **Дополнительными параметрами хэш-функции ГОСТ 3411 являются**	
	1. Стартовый вектор хэширования.	+
	2. Ключи для алгоритма симметричного шифрования ГОСТ 28147.	
	3. Начальное значение хэш-кода.	
	4. Начальный блок хэшируемого сообщения.	
14.	1. **Длина хэш-кода, создаваемого хэш-функцией SHA-1, равна**	
	1. 128 битов.	
	2. 160 битов.	+
	3. 512 битов.	
	4. 1024 битов.	
	2. **Длина блоков, на которые делится сообщение в хэш-функции SHA-1, равна**	
	1. 512 битов.	
	2. 1024 битов.	+
	3. 512 байтов.	
	4. 1024 байтов.	
	3. **Отметьте хэш-функции, хэш-код которых больше или равен 256 бит**	
	1. MD5.	
	2. ГОСТ 3411.	+
	3. SHA-1.	
	4. SHA-256.	+
	5. SHA-384.	+
	6. SHA-512.	+
15.	1. **Код аутентификации сообщения (MAC) может создаваться**	
	1. Только с использованием алгоритмов симметричного шифрования.	

	2. Только с использованием хэш-функций.	
	3. Как с использованием алгоритмов симметричного шифрования, так и с использованием хэш-функций.	+
	4. С помощью цифровой подписи.	
	2. **При разработке стандарта HMAC преследовались следующие цели**	
	1. Возможность использовать без модификаций уже имеющиеся хэш-функции.	+
	2. Возможность усилить алгоритм по сравнению с используемой им хэш-функцией.	
	3. Возможность легкой замены встроенных хэш-функций на более быстрые или более стойкие.	+
	4. Возможность не иметь общего секретного значения для обеспечения целостности передаваемого сообщения.	
	3. **При разработке стандарта HMAC преследовались следующие цели**	
	1. Сохранение скорости работы алгоритма обеспечения целостности, близкой к скорости работы используемой хэш-функции.	+
	2. Существенно увеличить скорость работы алгоритма обеспечения целостности по сравнению со скоростью работы используемой хэш-функцией.	
	3. Возможность использования секретных ключей и простота работы с ними.	+
	4. Возможность использования цифровых подписей.	
16.	1. **В стандарте HMAC для обеспечения целостности используется**	
	1. Хэширование исходного сообщения и секретного значения.	+
	2. Цифровая подпись исходного сообщения.	
	3. Алгоритм симметричного шифрования.	
	4. Хэширование исходного сообщения.	
	2. **В стандарте HMAC можно вести переговоры**	
	1. Об используемой хэш-функции.	+
	2. Об используемых константах.	
	3. Об используемых формулах преобразования.	
	4. Об используемой последовательности преобразований.	
	3. **Стандарт HMAC не позволяет вести переговоры**	

	1. Об используемой хэш-функции.	
	2. Об используемых константах.	+
	3. Об используемых формулах преобразования.	+
	4. Об используемой последовательности преобразований.	+

3. **Цифровая подпись, криптография с использованием эллиптических кривых, алгоритмы обмена ключей и протоколы аутентификации, Инфраструктура Открытого Ключа**

	1. **Функция, которую можно использовать в криптосистеме с открытым ключом, должна обладать следующими свойствами:**	
	1. Не иметь обратной функции.	
	2. Вычисление обратной функции должно иметь полиномиальную сложность без знания дополнительной информации.	
	3. Вычисление обратной функции должно иметь экспоненциальную сложность без знания дополнительной информации и полиномиальную сложность, если эта информация известна.	+
	4. Вычисление обратной функции должно иметь полиномиальную сложность без знания дополнительной информации и экспоненциальную сложность, если эта информация известна.	
	2. **Выберите правильное утверждение**	
	1. Цифровая подпись обеспечивает аутентификацию отправителя.	+
	2. Цифровая подпись обеспечивает конфиденциальность сообщения.	
	3. Цифровая подпись обеспечивает целостность сообщения.	+
	4. Цифровая подпись обеспечивает аутентификацию получателя.	
	3. **Выберите правильное утверждение**	
	1. Подпись должна быть битовым образцом, который зависит от подписываемого сообщения.	+
	2. Подпись должна использовать некоторую уникальную информацию отправителя для предотвращения подделки или отказа.	+
	3. Подпись должна обеспечивать невозможность просмотра сообщения.	
	4. Подпись должна обеспечивать невозможность восстановления исходного сообщения незаконным получателем.	
1.	1. **Подпись называется рандомизированной, если**	
	1. Для разных сообщений с использованием одного и того же закрытого	

	ключа при каждом подписывании создаются разные подписи.	
	2. Для одного и того же сообщения с использованием одного и того же закрытого ключа при каждом подписывании создаются разные подписи.	+
	3. Для одного и того же сообщения с использованием разных закрытых ключей при каждом подписывании создаются разные подписи.	
	4. Для разных сообщений с использованием разных закрытых ключей создаются разные подписи.	
	2. **Подпись называется детерминированной, если**	
	1. Для одного и того же сообщения с использованием разных закрытых ключей при каждом подписывании создается одна и та же подпись.	
	2. Для разных сообщений с использованием одного и того закрытого ключа при каждом подписывании создается одна и та же подпись.	
	3. Для одного и того же сообщения с использованием одного и того же закрытого ключа при каждом подписывании создается одна и та же подпись.	+
	4. Для разных сообщений с использованием разных закрытых ключей создаются разные подписи.	
	3. **Подпись, создаваемая алгоритмом DSS, называется**	
	1. Детерминированной.	
	2. Рандомизированной.	+
	3. Необратимой.	
	4. Корректной.	
2.	1. **В DSS используется хэш-функция**	
	1. MD5.	
	2. SHA-1.	+
	3. SHA-2.	
	4. ГОСТ-3411.	
	2. **Укажите, какая подпись является рандомизированной**	
	1. RSA.	
	2. DSS.	+
	3. ГОСТ 3410.	+
	4. AES.	

	3. **Укажите, какая подпись является детерминированной**	
	1. RSA.	+
	2. DSS.	
	3. ГОСТ 3410.	
	4. AES.	
3.	1. **Уравнение эллиптической кривой в общем случае имеет вид:**	
	1. $y^2 + axy + by = x^3 + cx^2 + dx + e$	+
	2. $y = ax^2 + bx + c$	
	3. $y^2 = ax^2 + bx + c$	
	2. **Криптография с использованием эллиптических кривых дает преимущества по сравнению с другими алгоритмами, потому что**	
	1. Принципиально не может быть взломана.	
	2. Обеспечивает эквивалентную защиту при меньшей длине ключа.	+
	3. Проще в реализации.	
	4. Может одновременно и подписывать сообщения, и шифровать их.	
	3. **Подпись с использованием эллиптических кривых имеет**	
	1. Один компонент.	
	2. Два компонента.	+
	3. Три компонента.	
	4. Четыре компонента.	
4.	1. **Выберите правильное утверждение:**	
	1. В криптографии с использованием эллиптических кривых все значения вычисляются по модулю n, где n – произведение двух простых чисел.	
	2. В криптографии с использованием эллиптических кривых все значения вычисляются по модулю простого числа p.	+
	3. В криптографии с использованием эллиптических кривых все значения вычисляются по модулю произвольного числа p.	
	2. **Задача, которую должен решить атакующий, формулируется следующим образом:**	

	1. Даны точки P и Q на эллиптической кривой E_p (a,b). Необходимо найти коэффициент k < p такой, что **P = k ×Q**	+
	2. Дана точка Q на эллиптической кривой E_p (a,b) и целое число k. Необходимо найти такую точку P на данной кривой, чтобы **P = k ×Q**	
	3. Дана точка P на эллиптической кривой E_p (a,b) и целое число k. Необходимо найти такую точку Q на данной кривой, чтобы **P = k ×Q**	
	3. **При использовании криптографии на эллиптических кривых в качестве аналога алгоритма Диффи-Хеллмана в уравнении $P_A = n_A \times G$**	
	1. Открытым ключом участника A является P_A, закрытым ключом участника A является n_A.	+
	2. Открытым ключом участника A является n_A, закрытым ключом участника A является P_A.	
	3. Открытым ключом участника A является P_A, закрытым ключом участника A является Q.	
5.	1. **Нулевым элементом эллиптической кривой считается точка O, которая**	
	1. имеет координаты (0, 0).	
	2. является бесконечно удаленной точкой, в которой сходятся все вертикальные прямые.	+
	3. имеет координаты (0, 1) или (1, 0).	
	2. **Шифрование/дешифрование с использованием эллиптических кривых выполняется следующим образом:**	
	1. Участник A выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение C_m, являющееся точкой на эллиптической кривой. **$C_m = \{k \times G, P_m + k \times P_B\}$**	+
	2. Участник A выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение C_m, являющееся точкой на эллиптической кривой. **$C_m = \{ P_m + k \times P_B\}$**	
	3. Участник A выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение C_m, являющееся точкой на эллиптической кривой. **$C_m = \{k \times G \}$**	
	3. **Элементами эллиптической кривой являются пары неотрицательных целых чисел, которые меньше простого числа p и удовлетворяют частному виду эллиптической кривой:**	

	1. $y \equiv x^2 + ax + b \pmod p$	
	2. $y^2 \equiv x^3 + ax + b \pmod p$	+
	3. $y^2 \equiv x^3 + ax^2 + b \pmod p$	
6.	1. **Выберите правильное высказывание**	
	1. Подпись с использованием эллиптических кривых является детерминированной.	
	2. Подпись с использованием эллиптических кривых является рандимизированной.	+
	3. Уравнения на эллиптических кривых нельзя использовать для создания цифровых подписей.	
	2. **Выберите правильное высказывание**	
	1. В криптографии с использованием эллиптических кривых нет аналога алгоритма Диффи-Хеллмана.	
	2. В криптографии с использованием эллиптических кривых есть аналог алгоритма Диффи-Хеллмана.	+
	3. Криптография с использованием эллиптических кривых не может использоваться для создания общего секрета.	
	3. **Выберите правильное высказывание**	
	1. Криптография с использованием эллиптических кривых может использоваться для шифрования сообщения.	+
	2. Криптография с использованием эллиптических кривых не может использоваться для шифрования сообщения.	
7.	1. **В уравнениях эллиптических кривых бесконечно удаленная точка, в которой сходятся все вертикальные прямые, называется**	
	1. Генерирующей точкой.	
	2. Нулевым элементом.	+
	3. Открытым ключом.	
	2. **При использовании криптографии на эллиптических кривых в качестве аналога алгоритма Диффи-Хеллмана в уравнении $P_A = n_A \times G$ точка G называется**	
	1. Генерирующей точкой.	+

	2. Нулевым элементом.	
	3. Открытым ключом.	
	3. **При использовании криптографии на эллиптических кривых в качестве аналога алгоритма Диффи-Хеллмана в уравнении $P_A = n_A \times G$ точка P_A называется**	
	1. Генерирующей точкой.	
	2. Нулевым элементом.	
	3. Открытым ключом.	+
8.	1. **Выберите правильное утверждение:**	
	1. Мастер-ключ должен быть более защищенным, чем ключ сессии.	+
	• Ключ сессии должен быть более защищенным, чем мастер-ключ.	
	• Мастер-ключ и ключ сессии должны иметь одинаковую степень защиты.	
	• **Nonce – это**	
	• Последовательный номер данной сессии.	
	• Случайное число, созданное специально для данной сессии.	+
	• Отметка времени.	
	• **Мастер-ключ используется для**	
	• Шифрования ключа сессии.	+
	• Шифрования прикладных данных.	
	• Шифрования как ключа сессии, так и прикладных данных.	
•	• **Под билетом понимается**	
	• Случайное число.	
	• Блок данных, зашифрованный секретным ключом, разделяемым каким-либо из участников и KDC.	+

	• Отметка времени.	
	• **Выберите правильное утверждение**	
	• Протоколы аутентификации используют только асимметричную криптографию.	
	• Протоколы аутентификации используют только симметричную криптографию.	
	• Протоколы аутентификации могут использовать как асимметричную, так и симметричную криптографию.	+
	• **Протокол аутентификации с использованием симметричного шифрования и билета для защиты от replay-атак использует**	
	• nonce	+
	• отметку времени	+
	• открытый ключ KDC.	
•	• **При односторонней аутентификации осуществляется аутентификация**	
	• Отправителя.	+
	• Получателя.	
	• KDC.	
	• **При односторонней аутентификации ключ сессии может шифроваться**	
	• Открытым ключом получателя.	+
	• Закрытым ключом отправителя.	
	• Мастер-ключом для симметричного шифрования, разделяемым отправителем и KDC.	+
	• **При односторонней аутентификации**	
	• Наличие KDC обязательно.	
	• Наличие KDC не обязательно.	+
•	• **В протоколе Нидхэма-Шредера KDC выполняет:**	

	• Аутентификацию участников.	+
	• Распределение ключа сессии.	+
	• Распределение открытых ключей участников.	
	• **В протоколе Нидхэма-Шредера защита от replay-атак выполняется с помощью**	•
	• отметки времени.	
	• последовательного номера.	
	• nonce.	+
	• **В протоколе Деннинга защита от replay-атак выполняется с помощью**	
	• отметки времени.	+
	• последовательного номера.	
	• nonce.	
•	• **Выберите правильное утверждение:**	
	• В протоколах аутентификации с использованием шифрования с открытым ключом участники должны знать открытый ключ AS или KDC.	+
	• В протоколах аутентификации с использованием шифрования с открытым ключом участники должны знать открытые ключи друг друга.	
	• В протоколах аутентификации с использованием шифрования с открытым ключом участники должны знать как открытый ключ AS или KDC, так и открытые ключи друг друга.	
	• **Выберите правильное утверждение:**	
	• В любом протоколе аутентификации ключ сессии всегда создается третьей доверенной стороной.	
	• В любом протоколе аутентификации ключ сессии всегда создается участником A.	
	• Существуют различные протоколы, в одних ключ сессии создается KDC, в других - одним из участников A или B.	+
	• **Под replay-атакой в данном контексте понимают:**	

	• Возможность взлома ключа сессии.	
	• Возможность использования старого ключа сессии.	+
	• Возможность взлома KDC.	

•	• **Сертификат открытого ключа имеет следующие характеристики**	
	• Любой участник, имеющий открытый ключ CA, может восстановить открытый ключ участника, для которого CA создал сертификат.	+
	• Никто, кроме сертификационного центра, выпустившего сертификат, не может подсмотреть сертификат.	
	• Никто, кроме сертификационного центра, выпустившего сертификат, не может незаметно модифицировать сертификат.	+
	• Любой участник, имеющий открытый ключ CA, может восстановить закрытый ключ участника, для которого CA создал сертификат.	
	• **Целью PKI является**	
	• Управление всем жизненным циклом сертификата открытого ключа.	+
	• Распределение ключей сессий между участниками.	
	• Предоставление доверенного и действительного открытого ключа участника.	+
	• Предоставление доверенного и действительного открытого ключа корневого сертификационного центра.	
	• **Сертификационный центр (CA) – это**	
	• Уполномоченный орган, который создает ключи сессии.	
	• Уполномоченный орган, который создает сертификаты открытого ключа.	+
	• Уполномоченный орган, который создает закрытые ключи.	
	• Уполномоченный орган, который определяет полномочия пользователей.	
•	• **Репозиторий сертификатов открытого ключа – это**	
	• База данных, в которой хранятся сертификаты и CRL.	
	• Система или набор распределенных систем, которые хранят сертификаты и CRL.	+
	• База данных, в которой хранится информация сертификационного центра.	
	• Система или набор распределенных систем, в которой хранится информация	

	сертификационного центра.	
	• **Цепочка сертификатов – это**	
	• Последовательность сертификатов, позволяющая определить действительность сертификата конечного участника.	+
	• Последовательность сертификатов, выпущенных данным сертификационным центром.	
	• Последовательность сертификатов некоторого конечного участника.	
	• Последовательность сертификатов, имеющихся у проверяющей стороны.	
	• **CRL – это**	
	• Список истекших сертификатов.	
	• Список отмененных сертификатов.	+
	• Список действительных сертификатов.	
	• Список самоподписанных сертификатов.	
•	• **Период действительности сертификата является интервалом времени, в течение которого CA гарантирует, что**	
	• Закрытый ключ участника не взломан.	
	• Информация в сертификате не изменилась.	
	• Сертификационный центр поддерживает информацию о статусе сертификата.	+
	• Пользователю не выданы другие сертификаты.	
	• **Поле Subject идентифицирует участника, который**	
	• Подписал данный сертификат.	
	• Является собственником сертификата и соответствующего закрытого ключа.	+
	• Является собственником закрытого ключа CA.	
	• Может иметь данный сертификат в своем хранилище сертификатов.	
	• **Расширения сертификата предоставляют методы**	
	• Для связывания дополнительных атрибутов с пользователями или открытыми ключами.	+
	• Для управления сертификатами.	+
	• Для указания дополнительных подписей сертификата.	

	• Для предотвращения подделки сертификата.	
•	• **Сертификат попадает в список отмененных сертификатов, если**	
	• Компрометирован закрытый ключ конечного участника.	+
	• Компрометирован закрытый ключ CA, выпустившего данный сертификат.	+
	• Истекло время действительности сертификата.	
	• Сертификат был украден.	
	• **Сертификат является самовыпущенным**	
	• Если **DN**, которые указаны в полях субъекта и выпускающего, являются пустыми.	
	• Если **DN**, которые указаны в полях субъекта и выпускающего, одинаковы и не пусты.	+
	• Если **DN**, которые указаны в полях субъекта и выпускающего, являются либо одинаковыми, либо пустыми.	
	• Если **DN**, которые указаны в полях субъекта и выпускающего, не совпадают.	
	• **Выберите правильное утверждение**	
	• Должно быть относительно легко создавать цифровую подпись.	+
	• Должно быть вычислительно невозможно подделать цифровую подпись как созданием нового сообщения для существующей цифровой подписи, так и созданием ложной цифровой подписи для некоторого сообщения.	+
	• Должно быть относительно легко проверять цифровую подпись.	+
	• Подпись обязательно должна быть рандомизированной.	

• **Протокол TLS/SSL**

•	• **Целями протокола SSL/TLS являются**	
	• Интероперабельность.	+
	• Предотвращение атак «man-in-the-middle».	+
	• Предотвращение DoS-атак.	
	• Относительная эффективность.	+
	• **Целями протокола SSL/TLS являются**	
	• Расширяемость.	+

	• Криптографическая безопасность.	+
	• Предотвращение DDoS-атак.	
	• Предоставление сервисов для биллинга.	
	• **Протокол SSL/TLS предоставляет сервисы безопасности для**	
	• Прикладного протокола.	+
	• Транспортного протокола.	
	• Протокола канального уровня.	
	• Протокола физического уровня.	
•	• **Расширяемость в протоколе SSL/TLS обеспечивается тем, что**	
	• SSL/TLS определяет общий каркас (framework), в который могут быть встроены новые алгоритмы открытого ключа и симметричного шифрования.	+
	• SSL/TLS имеет фиксированный набор алгоритмов симметричного шифрования и определяет каркас (framework), в который могут быть встроены новые алгоритмы открытого ключа.	
	• SSL/TLS имеет фиксированный набор алгоритмов открытого ключа и определяет каркас (framework), в который могут быть встроены новые алгоритмы симметричного шифрования.	
	• SSL/TLS имеет фиксированный набор алгоритмов симметричного шифрования и алгоритмов открытого ключа.	
	• **Относительная эффективность в протоколе SSL/TLS обеспечивается тем, что**	
	• Вводится понятие сессии, в рамках которой может быть создано несколько TCP-соединений.	+
	• Не используется криптография с открытым ключом, требующая больших вычислений.	
	• В качестве транспортного протокола используется UDP, который более быстро устанавливает соединение. Надежность соединения обеспечивается на уровне SSL/TLS.	
	• Для обеспечения конфиденциальности используются более быстрые алгоритмы симметричного шифрования с меньшей длиной ключа.	
	• **Протокол SSL/TLS имеет**	
	• Один уровень.	
	• Два уровня.	+
	• Три уровня.	
	• Четыре уровня.	
•	• **Протокол Записи в SSL/TLS обеспечивает**	

	• Аутентификацию клиента.	
	• Конфиденциальность соединения.	+
	• Целостность соединения.	+
	• Аутентификацию сервера.	
	• **Протокол Записи используется**	
	• Для инкапсуляции различных протоколов более высокого уровня.	+
	• Для инкапсуляции только HTTP-протокола.	
	• Для инкапсуляции только протокола Рукопожатия.	
	• Для инкапсуляции TCP-протокола.	
	• **Взаимное расположение протоколов Записи и Рукопожатия с стеке протоколов**	
	• Протокол Рукопожатия использует протокол Записи в качестве транспорта для ведения переговоров о параметрах безопасности.	+
	• Протокол Записи использует протокол Рукопожатия в качестве транспорта для ведения переговоров о параметрах безопасности.	
	• Протоколы Рукопожатия и Записи расположены на одном уровне в стеке протоколов и выполняются поверх протокола TCP.	
	• Протоколы Рукопожатия и Записи расположены на одном уровне в стеке протоколов и выполняются поверх протокола IP.	
•	• **Протокол Рукопожатия обеспечивает безопасность соединения, используя следующие сервисы**	
	• Участники аутентифицированы с использованием криптографии с открытым ключом.	+
	• Для аутентификации участников используется Третья Доверенная Сторона, сертификат которой имеет каждый участник.	
	• Переговоры о разделяемом секрете надежны.	
	• Участники аутентифицированы с использованием общего секрета или криптографии с открытым ключом.	
	• **Протокол Рукопожатия обеспечивает безопасность соединения, используя следующие сервисы**	
	• Переговоры о разделяемом секрете надежны, если выполнена аутентификация хотя бы одной из сторон.	+
	• Для аутентификации участников используется Третья Доверенная Сторона, с которой участники имеют общий секрет.	
	• Переговоры об используемых алгоритмах шифрования безопасны, т.е. их нельзя подсмотреть.	

	• Переговоры о разделяемом секрете безопасны, т.е. этот секрет нельзя подсмотреть.	+
	• **Выберите правильное утверждение**	
	• В протоколе SSL/TLS участники аутентифицируются с использованием криптографии с открытым ключом.	+
	• В протоколе SSL/TLS участники аутентифицируются с использованием разделяемого секрета.	
	• В протоколе SSL/TLS сервер аутентифицирует себя с использованием криптографии с открытым ключом, аутентификация клиента выполняется по паролю.	
	• В протоколе SSL/TLS сервер аутентифицирует себя по паролю, аутентификация клиента выполняется с использованием криптографии с открытым ключом.	
•	• **Под безопасностью переговоров о разделяемом секрете понимается**	
	• Разделяемый общий секрет невозможно подсмотреть.	+
	• Разделяемый общий секрет невозможно изменить.	
	• Невозможно узнать алгоритмы, для которых создается разделяемый общий секрет.	
	• Невозможно узнать режимы выполнения алгоритмов, для которых создается разделяемый общий секрет.	
	• **Под надежностью переговоров о разделяемом секрете понимается**	
	• Атакующий, расположенный в середине соединения, не может модифицировать передаваемый секрет незаметно для участников соединения.	+
	• Атакующий, расположенный в середине соединения, не может подсмотреть передаваемый секрет.	
	• Атакующий, расположенный в середине соединения, не может узнать алгоритм, с использованием которого передается секрет.	
	• Атакующий, расположенный в середине соединения, не может узнать алгоритм, для использования в котором передается секрет.	
	• **Содержимым протокола Alert в SSL/TLS является**	
	• Фатальное сообщение о закрытии соединения.	
	• Либо фатальное, либо предупреждающее сообщение.	+
	• Предупреждающее сообщение.	
	• Сообщение, показываемое пользователю для ввода логина и пароля пользователя.	
•	• **Протокол Записи выполняет следующее**	
	• Фрагментирует сообщение на блоки нужной длины.	+

	• Осуществляет сжатие данных.	+
	• Аутентифицирует сервер.	
	• Подписывает передаваемые данные.	
	• **Протокол Записи выполняет следующее**	
	• Вычисляет HMAC.	+
	• Зашифровывает данные.	+
	• Аутентифицирует клиента.	
	• Согласовывает общий секрет.	
	• **В протоколе SSL/TLS функция PRF**	
	• Создает случайную последовательность битов.	
	• Вырабатывает мастер-секрет.	
	• Расширяет мастер-секрет до нужной длины для создания всех необходимых ключей.	+
	• Увеличивает длину мастер-секрета в два раза.	
•	• **Состояние соединения в протоколе SSL/TLS**	
	• Определяет параметры выполнения протокола Записи.	+
	• Определяет способ аутентификации клиента.	
	• Определяет способ аутентификации сервера.	
	• Определяет прикладной протокол, который выполняется выше протокола Записи.	
	• **Параметрами соединения в протоколе SSL/TLS являются**	
	• Алгоритм сжатия.	+
	• Алгоритм шифрования.	+
	• Пароль клиента.	
	• Сертификат сервера.	
	• **Параметрами соединения в протоколе SSL/TLS являются**	
	• MAC-алгоритм.	+

	• Секреты MAC, ключи алгоритма шифрования и инициализационные вектора.	+
	• Идентификатор клиента.	
	• Сертификат клиента.	
•	• **Определены следующие состояния соединения**	
	• Текущее состояние чтения.	+
	• Текущее состояние записи.	+
	• Ожидаемое состояние чтения.	+
	• Ожидаемое состояние записи.	+
	• **Параметры безопасности для ожидаемых состояний устанавливаются**	
	• Протоколом Рукопожатия.	+
	• Протоколом HTTP.	
	• Протоколом TCP.	
	• Протоколом IP.	
	• **Протокол изменения шифрования**	
	• Делает ожидаемое состояние текущим, в результате чего соответствующие параметры текущего состояния сбрасываются и заменяются параметрами ожидаемого состояния.	+
	• Делает ожидаемое состояние текущим, в результате чего соответствующие параметры текущего состояния заменяются параметрами ожидаемого состояния, а параметры ожидаемого состояния – параметрами текущего.	
	• Делает ожидаемое состояние текущим, в результате чего параметры текущего и ожидаемого состояний сбрасываются.	
	• Делает ожидаемое состояние текущим, в результате чего соответствующие параметры ожидаемого состояния сбрасываются и заменяются параметрами текущего состояния.	
•	• **Из мастер-секрета создаются следующие данные**	
	• Ключи MAC, разные в обоих направлениях.	+
	• Ключи для алгоритма симметричного шифрования, разные в обоих направлениях.	+
	• Сертификаты сервера.	
	• Инициализационные вектора для алгоритма симметричного шифрования, одинаковые в обоих направлениях.	
	• **Из мастер-секрета создаются следующие данные**	

	• Инициализационные вектора для алгоритма симметричного шифрования, разные в обоих направлениях.	+
	• Сертификаты клиента.	
	• Ключи для алгоритма симметричного шифрования, одинаковые в обоих направлениях.	
	• Признак возобновляемости сессии.	
	• **Параметры безопасности в протоколе SSL/TLS для ожидаемых состояний устанавливаются**	
	• Протоколом Рукопожатия.	+
	• Протоколом Записи.	
	• Центром распределения ключей (KDC).	
	• Протоколом прикладного уровня.	
•	• **Протокол Рукопожатия в SSL/TLS обязательно включает следующие шаги**	
	• Обмен сообщениями **Hello** клиента и сервера.	+
	• Посылка сертификата сервера.	
	• Обмен сообщениями для выработки общего секрета.	+
	• Посылка сертификата клиента.	
	• **Сообщения Hello в протоколе SSL/TLS обеспечивают**	
	• Согласование используемых алгоритмов.	+
	• Обмен случайными значениями.	+
	• Проверку возобновляемости сессии.	+
	• Аутентификация сервера.	
	• **Протокол Рукопожатия в SSL/TLS может не включать следующие шаги**	
	• Обмен сообщениями **Hello** клиента и сервера.	
	• Посылку сертификата сервера.	+
	• Посылку сертификата клиента.	+
	• Обмен сообщениями для выработки общего секрета.	
•	• **Выберите правильное утверждение**	

	• В протоколе SSL/TLS первым выполняет аутентификацию клиент.	
	• В протоколе SSL/TLS первым выполняет аутентификацию сервер.	+
	• В протоколе SSL/TLS аутентификация клиента и сервера выполняется одновременно с использованием Третьей Доверенной стороны.	
	• В протоколе SSL/TLS никогда не выполняется ни аутентификация клиента, ни аутентификация сервера.	
	• **Выберите правильное утверждение**	
	• В протоколе SSL/TLS только аутентифицированный клиент может запросить сертификат сервера.	
	• В протоколе SSL/TLS только аутентифицированный сервер может запросить сертификат клиента.	+
	• В протоколе SSL/TLS аутентификация и клиента, и сервера является обязательной.	
	• В протоколе SSL/TLS никогда не выполняется ни аутентификация клиента, ни аутентификация сервера.	
	• **Сокращенное Рукопожатие в протоколе SSL/TLS позволяет**	
	• Увеличить производительность протокола SSL/TLS.	+
	• Повысить безопасность протокола SSL/TLS.	
	• Повысить интероперабельность протокола SSL/TLS.	
	• Повысить надежность протокола SSL/TLS.	
•	• **Расширения SSL/TLS предназначены для обеспечения следующих возможностей**	
	• Позволить серверам запрашивать авторизационную информацию клиента.	
	• Позволить клиентам указывать имя виртуального сервера.	+
	• Позволить SSL/TLS максимально эффективно функционировать в новых окружениях с ограниченными возможностями.	+
	• Использовать новые криптографические алгоритмы.	
	• **Обратная совместимость при использовании расширений SSL/TLS означает**	
	• Клиенты версии TLS 1.0, которые поддерживают расширения, могут общаться с серверами TLS 1.0, не поддерживающими расширения.	+
	• Клиенты версии TLS 1.0, которые не поддерживают расширения, могут общаться с серверами TLS 1.0, поддерживающими расширения.	+
	• При использовании расширений следует устанавливать дополнительное ПО на стороне клиента.	

	• При использовании расширений следует устанавливать дополнительное ПО на стороне сервера.	
	• **Сообщение Finished протокола SSL/TLS посылается**	
	• Для проверки успешного завершения обмена ключа и процессов аутентификации.	+
	• Для завершения используемого транспортного протокола.	
	• Для указание использовать новые алгоритмы и ключи.	
	• Для аутентификации клиента.	

Список вопросов для индивидуального собеседования на промежуточной аттестации.

1. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; классификация атак.
2. Алгоритмы симметричного шифрования. Понятие стойкости алгоритма, типы операций, используемых в алгоритмах симметричного шифрования. Сеть Фейштеля.
3. Алгоритмы DES и тройной DES.
4. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147.
5. Режимы выполнения алгоритмов симметричного шифрования. Способы создания псевдослучайных чисел.
6. Алгоритм Rijndael. Математические понятия, лежащие в основе алгоритма Rijndael. Структура алгоритма Rijndael.
7. Основные понятия, относящиеся к криптографии с открытым ключом, способы использования алгоритмов с открытым ключом: шифрование, создание и проверка цифровой подписи, обмен ключа.
8. Алгоритм RSA.
9. Алгоритм Диффи-Хеллмана.
10. Требования к криптографическим хэш-функциям. Хэш-функции MD5, SHA-1, SHA-2, SHA-3 и ГОСТ 3411.
11. Обеспечение целостности сообщений.
12. Основные требования к цифровым подписям, стандарты цифровой подписи ГОСТ 3410 и DSS.
13. Криптография с использованием эллиптических кривых.
14. Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны.
15. Аутентификация и обмен ключей в протоколе Kerberos.
16. Инфраструктура открытого ключа. Сертификаты X.509 v3.
17. Инфраструктура открытого ключа. Репозиторий сертификатов. Способы отмены сертификатов.
18. Аутентификация и обмен ключей в протоколе TLS/SSL.
19. Классификация межсетевых экранов. Пакетные фильтры с поддержкой и без поддержки состояния.
20. Понятие DMZ. Различные топологии DMZ сетей с использованием межсетевых экранов разного типа.
21. Способы классификации систем обнаружения вторжений (IDS).

22. Принципы безопасного развертывания сервисов DNS. Защита транзакций с использованием HMAC (стандарт TSIG).
23. Безопасность DNS Query / Response (стандарт DNSSEC).
24. Технологии аутентификации в веб.
25. Безопасность веб: технологии активного содержимого на стороне сервера и связанные с этим уязвимости.
26. Основные превентивные средства обеспечения безопасности веб-приложений.
27. Основные типы SQL-injection.
28. Основные возможности межсетевого экрана прикладного уровня для протокола HTTP (WAF) ModSecurity.
29. Аутентификация и обмен ключей в протоколе SSH.
30. Протокол GRE и протоколы канального уровня PPP и L2TP.
31. Семейство протоколов IPSec. Протоколы AH и ESP.
32. Семейство протоколов IPSec. Аутентификация сторон и обмен ключа в протоколе IKE.
33. Технологии создания единого входа, стандарт SAML.
34. Способы управления доступом, дискреционный и мандатный способы управления доступом, RBAC.

Приложение 1.

СИСТЕМА РЕЙТИНГОВОЙ ОЦЕНКИ И КОНТРОЛЯ ЗНАНИЙ СТУДЕНТОВ

№ п/п	СТРУКТУРА	Баллы по каждому модулю
1.	Оценка за активное участие в учебном процессе и посещение занятий: Всех занятий Не менее 75% Не менее 50% Не менее 25% Итого:	 5 4 3 2 до 5
2.	устный опрос в форме собеседования (УО-1) письменный опрос в виде теста (ПР-1) письменная контрольная работа (ПР-2) устный опрос в форме коллоквиума (УО-2) письменная работа в форме реферата (ПР-4) Итого:	5 10 10 10 10 45
3.	Зачет	50
	ВСЕГО:	100

Пересчет на 5 балльную систему

2 (неудовлетворительно)	3 (удовлетворительно)	4 (хорошо)	5 (отлично)
< 50	**50-64**	**65-84**	**85-100**

Язык преподавания: русский.

Автор (авторы) программы: к.ф..м.н., доцент факультета ВМК МГУ имени М.В. Ломоносова И.Н Смирнов.

Преподаватель (преподаватели) программы: к.ф..м.н., доцент факультета ВМК МГУ имени М.В. Ломоносова И.Н Смирнов.