Автономная некоммерческая организация высшего образования
«Международный банковский институт имени Анатолия Собчака»

УТВЕРЖДАЮ

Ректор _____ *Сигова М.В.*

"___" _____ 20___ г.

Рабочая программа дисциплины «Информационная безопасность»

Специальность: *38.05.01 Экономическая безопасность*

Специализация: *Экономико-правовое обеспечение экономической безопасности*

Уровень образовательной программы: *специалитет*

Форма обучения: *очная*

Составитель: Пискунова Т.Г.

Санкт-Петербург
2021

ВВОДНАЯ ЧАСТЬ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Информационная безопасность» являются формирование у обучающихся теоретических знаний в области защиты информации, приобретение практических навыков обеспечения информационной безопасности, применение на практике полученных знаний и умений в соответствии с международными требованиями к избранному виду деятельности.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с установленными в образовательной программе индикаторами достижения компетенций, представлены в таблице 1.

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП

3.1. Дисциплина «Информационная безопасность» относится к дисциплинам по выбору учебного плана образовательной программы.

Таблица 1

Планируемые результаты обучения по дисциплине, соотнесенные с установленными в образовательной программе индикаторами достижения

Код и наименование компетенции выпускника	Код и наименование индикаторов достижения компетенций	Планируемые результаты обучения по дисциплине
1	2	3
ПК-4. Способен анализировать и объединять потенциальные возможности управления рисками с точки зрения социального, экономического, нормативно-законодательного, экологического и технологического контекста для создания долгосрочной стоимости	ПК-4.1. Применяет международные и национальные стандарты обеспечения социальной ответственности и регулирования вопросов устойчивого развития.	**Знать:** основные понятия и определения, используемые при изучении информационной безопасности. **Уметь:** анализировать способы нарушения информационной безопасности. **Владеть:** навыками разработки концепции информационной безопасности предприятия.
	ПК-4.2. Определяет наиболее важные для функционирования организации (социально-экономической системы) направления, технические и социально-экономические процессы.	**Знать:** классификацию угроз информационной безопасности. **Уметь:** определять виды возможных нарушений в информационной системе. **Владеть:** навыками разработки программы информационной безопасности предприятия.
	ПК-4.3. Анализирует и научно обосновывает общую стратегию организации, социально-экономической системы, стратегии по отдельным видам и направлениям деятельности, проектам, про-	**Знать:** основные цели, задачи и принципы защиты конфиденциальной компьютерной информации. **Уметь:** правильно оценивать степень важности информации, подлежащей защите. **Владеть:** навыками разработки политики информационной безопасности предприятия.

	цессам.	
ПК-9. Способен разрабатывать, формулировать технические задания и управлять проектами технико-информационного обеспечения системы управления рисками	ПК-9.1. Демонстрирует знание сущности и принципов управления проектами.	**Знать:** классификацию компьютерных вирусов и правила защиты от них. **Уметь:** правильно выбирать необходимый уровень защиты информации от несанкционированного доступа. **Владеть:** способностью применять на практике международные и российские профессиональные стандарты информационной безопасности.
	ПК-9.2. Ставит цели и формулирует задачи, связанные с реализацией профессиональных функций работников.	**Знать:** принципы разработки вычислительно стойких шифров для практических криптосистем закрытия коммерческой информации. **Уметь:** выбирать соответствующие средства защиты. **Владеть:** навыками обобщения, интерпретации полученных результатов по заданным или определенным критериям.
	ПК-9.3. Разрабатывает требования к программному обеспечению по управлению рисками, оказывает помощь в выборе автоматизированной системы управления рисками.	**Знать:** характеристики и алгоритмы работы важнейших современных аппаратно-программных средств защиты компьютерной информации в сфере обеспечения информационной безопасности. **Уметь:** эффективно использовать на практике современные методы и средства криптографической защиты конфиденциальной информации. **Владеть:** автоматизированными системами управления рисками.
	ПК-9.4. Осуществляет постановку задач и контроль внедрения информационной системы управления рисками.	**Знать:** законодательную и нормативную базу информационной безопасности; перспективы развития технологий обеспечения информационной безопасности. **Уметь:** оформлять, представлять, описывать, характеризовать данные, сведения, факты, результаты работы. **Владеть:** методами внедрения информационной системы управления рисками.

ОСНОВНАЯ ЧАСТЬ
1. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Распределение трудоемкости учебной дисциплины по видам работ по семестрам для очной формы обучения

Вид учебной работы	Трудоемкость			
	зач. ед.	час.	по семестрам	
			9	А
Общая трудоемкость дисциплины по учебному плану	**3**	**108**	**108**	
Контактная работа, в том числе:		**40**	**40**	
Аудиторные занятия		**40**	**40**	
Лекции (Л)		16	16	
Практические занятия (ПЗ)		24	24	
Самостоятельная работа (СРС)		**68**	**68**	
в том числе:				
курсовая работа (проект)				
в том числе:				
контактная работа (индивидуальные консультации и защита курсовой работы)				
контрольные работы (по учебному плану)				
Экзамен				
в том числе:				
контактная работа (консультации перед экзаменом)				
Дифференцированный зачет		4	4	

2. СОДЕРЖАНИЕ РАЗДЕЛОВ ДИСЦИПЛИНЫ

Тематический план, структурированный по видам учебных занятий с указанием их объемов в соответствии с учебным планом

№	Наименование темы учебной деятельности, включая самостоятельную работу обучающихся (в час.)	Виды учебной деятельности, включая самостоятельную работу обучающихся в часах				Форма текущего контроля успеваемости
		Л	ПЗ	СР	всего	
1	Постановка задачи обеспечения информационной безопасности	1	2	2	5	тесты
2	Основные понятия и определения в данной области	1	2	2	5	тесты
3	Стандарты информационной безопасности	1	2	8	11	тесты
4	Обзор основных технологий защиты информационных систем	1	2	8	11	тесты
5	Защита от вирусов	2	4	8	14	тесты
6	Межсетевые экраны	2	2	8	12	тесты
7	Виртуальные частные сети	2	2	8	12	тесты
8	Основные методы криптографической защиты	2	2	8	12	тесты
9	Алгоритмы построения современных	2	2	8	12	тесты

	шифров с симметричными и асимметричными ключами					
10	Возможности применения методов криптографии для обеспечения безопасности электронных платежей	2	4	8	14	тесты
	Дифференцированный зачет				4	
	ИТОГО	16	24	68	108	

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1.Содержание лекционных, практических занятий. Содержание самостоятельной работы.

Тема 1 Постановка задачи обеспечения информационной безопасности

Лекция. Основные положения теории информационной безопасности информационных систем. Цели и задачи информационной безопасности. Понятие угрозы. Виды противников или «нарушителей».

Практическое занятие. Методы и средства защиты информации.

Самостоятельная работа. Теоретическая подготовка: изучение материала лекционных занятий.

Темы эссе: Компьютерная преступность в зарубежном законодательстве. Компьютерная преступность в российском законодательстве. Персональные данные и Интернет. Защита баз данных.

Тема 2 Основные понятия и определения в данной области

Лекция. Разработка концепции информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Информационная безопасность в условиях функционирования в России глобальных систем.

Практическое занятие. Методика оценки уровня информационной безопасности.

Самостоятельная работа. Теоретическая подготовка: изучение материала лекционных занятий.

Темы эссе: Международные стандарты информационной безопасности. Российские стандарты информационной безопасности. Политика информационной безопасности организации. Обеспечение безопасности операционных систем.

Тема 3 Стандарты информационной безопасности

Лекция. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Международные стандарты информационного обмена.

Практическое занятие. Функциональные возможности программы GNUPT.

Самостоятельная работа. Теоретическая подготовка: изучение материала лекционных занятий.

Темы эссе: Безопасность функционирования международной системы SWIFT. Мошенничество в сети Интернет. Промышленный шпионаж в сети Интернет. Конкурентная разведка в сети Интернет. Политика информационной безопасности организации. Проблемы соблюдения авторских прав в сети Интернет. Обеспечение правовой охраны компьютерных программ

Тема 4 Обзор основных технологий защиты информационных систем

Лекция. Три вида возможных нарушений информационной системы. Анализ способов нарушений информационной безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Практическое занятие. Основные характеристики МСЭ.

Самостоятельная работа. Теоретическая подготовка: изучение материала лекционных занятий.

Темы эссе: Алгоритм организации секретной связи без опубликования ключей. Итерационные блочные шифры. Криптосхема Фейстеля. Сертификация открытых ключей. Сертификационный центр.

Тема 5 Защита от вирусов

Лекция. Типы компьютерных вирусов. Что такое компьютерный вирус. Классификация вирусов. Борьба с компьютерными вирусами. Современные антивирусные программы; предъявляемые к ним требования.

Практическое занятие. Сравнение российских VPN.

Самостоятельная работа. Теоретическая подготовка: изучение материала лекционных занятий.

Темы эссе: Применение расширенного алгоритма Евклида для расчета секретного ключа в алгоритме RSA. Способы организации секретной связи.

Тема 6 Межсетевые экраны

Лекция. Межсетевые экраны: основные понятия, классификация, программная и аппаратная реализация.

Практическое занятие. ЭЦП на основе алгоритма Эль-Гамаля.

Самостоятельная работа. Теоретическая подготовка: изучение материала лекционных занятий.

Темы эссе: Безопасность облачных вычислений. Биометрическая аутентификация пользователя

Правовое регулирование электронного документооборота. Персональные данные и Интернет. Защита баз данных. Защита информации в социальных сетях

Тема 7 Виртуальные частные сети

Лекция. Виртуальные частные сети: назначение, способы реализации.

Практическое занятие. Алгоритмы Диффи-Хеллмана и Хилла.

Самостоятельная работа. Теоретическая подготовка: изучение материала лекционных занятий.

Темы эссе: Режимы шифрования блочных шифров. Режим CDC и его свойств. Режим шифрования OFB и его свойства.

Тема 8 Основные методы криптографической защиты

Лекция. Криптология: криптография и криптоанализ; основные используемые понятия и определения. Основы криптографии. Виды атак на шифр.

Практическое занятие. Криптоанализ симметричных и асимметричных шифров.

Самостоятельная работа. Теоретическая подготовка: изучение материала лекционных занятий.

Темы эссе: Пакет программ «Криптон-шифрование». Архивное шифрование и его реализация. Криптология: основные понятия.

Тема 9 Алгоритмы построения современных шифров с симметричными и асимметричными ключами

Лекция. Принципы построения алгоритма шифрования. Использование шифрующей сети для построения алгоритма. Общая структура алгоритма шифрования по ГОСТ 28147-89. Сущность электронной цифровой подписи.

Практическое занятие. Алгоритмы шифрования.

Самостоятельная работа. Теоретическая подготовка: изучение материала лекционных занятий.

Темы эссе: Сетевое шифрование и его реализация. Виды атак на шифр.

Тема 10 Возможности применения методов криптографии для обеспечения

безопасности электронных платежей

Лекция. Протоколы безопасных электронных платежей. Протокол SSL (Secure Socket Layer). Протокол безопасных транзакций в сети Интернет – протокол SET.

Практическое занятие. Криптоанализ хэш-функций.

Самостоятельная работа. Теоретическая подготовка: изучение материала лекционных занятий.

Темы эссе: Хэш-функция: назначение, требования, свойства. Методы криптографии для обеспечения безопасности электронных платежей.

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Аудиторная работа

Основными видами аудиторной работы обучающихся являются лекции и практические занятия.

В ходе **лекций** преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, даёт рекомендации на практическое занятие и указания на самостоятельную работу.

Практические занятия завершают изучение тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки сообщений по проблематике, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности обучающихся по изучаемой дисциплине.

Практическое занятие предполагает свободный обмен мнениями по избранной тематике. Он начинается со вступительного слова преподавателя, формулирующего цель занятия и характеризующего его основную проблематику. Затем, как правило, заслушиваются сообщения обучающихся. Обсуждение сообщения совмещается с рассмотрением намеченных вопросов. Сообщения, предполагающие анализ публикаций по отдельным вопросам практического занятия, заслушиваются обычно в середине занятия. Поощряется выдвижение и обсуждение альтернативных мнений.

Качество учебной работы обучающихся преподаватель оценивает в конце практического занятия, выставляя в рабочий журнал текущие оценки.

Консультации проводятся для всех обучающихся по предварительной договоренности с преподавателем и в рамках графика проведения консультаций. С графиком проведения консультаций преподавателя можно ознакомиться на кафедре.

Самостоятельная работа

Самостоятельная работа – изучение материала лекционных занятий и рекомендованной литературы, выполнение заданий преподавателя, а также проработка отдельных тем и аспектов дисциплины в виде докладов и сообщений, подготовка к промежуточной аттестации.

Промежуточная аттестация

Изучение дисциплины заканчивается промежуточной аттестацией, которая проводится по всему ее содержанию. Форма промежуточной аттестации, предусмотренная учебным планом – дифференцированный зачет.

К промежуточной аттестации допускаются обучающиеся, которые систематически, в течение всего семестра работали на занятиях и показали уверенные знания по вопросам, выносившимся на групповые занятия.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ПО ДИСЦИПЛИНЕ

5.1.Пояснительная записка

В соответствии с требованиями ФГОС ВО по специальности Экономическая безопасность для проведения текущего контроля успеваемости и промежуточной аттестации дисциплины «Информационная безопасность» разработаны оценочные средства по данной дисциплине, являющиеся неотъемлемой частью учебно-методической ее документации в рамках реализуемой Основной образовательной программы.

5.2. Оценочные средства промежуточной аттестацию по дисциплине

Формой промежуточной аттестации по дисциплине является – дифференцированный зачет

Вопросы для проведения промежуточной аттестации:

1. Принципы построения шифров с симметричным ключом. Шифры замены.
2. Применение расширенного алгоритма Евклида для расчета секретного ключа в алгоритме RSA.
3. Способы организации секретной связи. Цели и задачи защиты информации.
4. Пакет программ «Криптон-шифрование»; архивное шифрование и его реализация.
5. Криптология. Основные понятия.
6. Пакет программ «Криптон-шифрование»; сетевое шифрование и его реализация.
7. Атаки на шифр. Виды атак на шифр.
8. Алгоритм Диффи-Хеллмана.
9. Система секретной связи Шеннона. Абсолютно стойкий и условно стойкий шифры.
10. Алгоритм шифрования RSA.
11. Шифры перестановки.
12. Бинарный алгоритм возведения в дискретную степень по модулю.
13. Построение блочных шифров симметричного шифрования.
14. ЭЦП и схема ее практической реализации.
15. Шифр с управляемыми подстановками.
16. Алгоритм организации секретной связи без опубликования ключей.
17. Итерационные блочные шифры. Криптосхема Фейстеля.
18. Сертификация открытых ключей. Сертификационный центр.
19. Режимы шифрования блочных шифров. Режим CDC и его свойства.
20. Хэш-функция: назначение, требования, свойства.
21. Режим шифрования OFB и его свойства.
22. Хэш-функция по ГОСТ Р 34.41-94, структурная схема; описание работы.
23. Режим шифрования CFB и его свойства.
24. Шифры с управляемыми перестановками.
25. Алгоритм шифрования ГОСТ 28147-84.
26. Смарт-карты; их свойства.
27. Пакет «Криптон-шифрование». Ключевые схемы пользователя и их применение.
28. Типы аутентификации информации. Протокол аутентификации Kerberos.

5.3. Текущий контроль успеваемости

Текущий контроль успеваемости обучающихся по дисциплине проводится в форме контрольных мероприятий: тренировочного тестирования, выполнения практических заданий.

Активность обучающегося на занятиях оценивается на основе выполненных работ и заданий, предусмотренных рабочей программой дисциплины. Обучающемуся, пропустившему практические занятия, необходимо выполнить задания самостоятельно и защитить их выполнение перед преподавателем практических занятий.

5.3.1. Тестовые задания по дисциплине (примеры)

Название темы	Пример теста

дисциплины	
Основные понятия и определения в данной области	Политика безопасности – это совокупность норм, правил и методов, на основе которых строится работа информационной системы в области Выберите хотя бы один ответ. ☐ a. оценки критичной информации ✗ ☑ b. обращения критичной информации ✓ ☑ c. распределения критичной информации ✓ ☐ d. анализа критичной информации ✗ ☑ e. хранения критичной информации ✓
Обзор основных технологий защиты информационных систем	Инженерно-технические меры обеспечения безопасности банковских информационных систем включают: Выберите хотя бы один ответ. ☑ a. Средства физической защиты компьютерных систем ✓ ☑ b. Устройства предотвращения похищения техники из информационных центров ✓ ☑ c. Аппаратные средства криптографической защиты ✓ ☐ d. Регламентация всех технологических процессов ✗ ☐ e. Меры физической защиты компьютерных систем ✗
Защита от вирусов	Какие из указанных качеств не имеют отношения к монитору обращений? Выберите хотя бы один ответ. ☐ a. Полнота ✗ ☐ b. Верифицируемость ✗ ☑ c. Функциональность ✓ ☐ d. Изолированность ✗

	☑ e. Независимость ✓
Межсетевые экраны	Межсетевой экран выполняет функции Выберите один ответ. ◉ a. преобразования некоторых элементов передаваемых даых ✓ ○ b. очистки некоторых элементов передаваемых данных ✗ ○ c. пополнения некоторых элементов, передаваемых данных ✗
Виртуальные частные сети	Защита информации в процессе ее передачи по туннелю VPN основана на выполнении следующих функций: Выберите хотя бы один ответ. ☑ a. аутентификация взаимодействующих сторон ✓ ☑ b. проверка подлинности и целостности доставляемой информации. ✓ ☐ c. разрешение или запрещение дальнейшей передачи данных ✗

5.3.2. Критерии оценивания результатов обучения по дисциплине:

Знания, умения и навыки обучающихся при промежуточном контроле в форме дифференцированного зачета определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

1. «Отлично» — обучающийся глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, не затрудняется с ответом при видоизменении задания, свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, умеет самостоятельно обобщать и излагать материал, не допуская ошибок.

2. «Хорошо» — обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми умениями и навыками при выполнении практических заданий.

3. «Удовлетворительно» — обучающийся усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий.

4. «Неудовлетворительно» — обучающийся не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические задания, задачи.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

При подготовке к занятиям и для выполнения индивидуальных заданий следует использовать рекомендуемые источники литературы по данному курсу, в том числе нормативные документы. При подготовке к занятиям следует воспользоваться не только учебниками и учебными пособиями, приведенными в списке основной и дополнительной рекомендуемой литературы, но также периодическими изданиями**.**

6.1. Основная литература

1. Основы информационной безопасности : учебник для студентов вузов / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва : ЮНИТИ-ДАНА, 2017. — 287 с. — ISBN 978-5-238-02857-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/72444.html

6.2. Дополнительная литература

1. Сафонова, Л. А. Экономические аспекты информационной безопасности : учебное пособие / Л. А. Сафонова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2019. — 97 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/90606.html

2. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 54 с. — ISBN 978-5-4487-0298-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/77320.html

3. Ванина, М. Ф. Защита информации и контроль данных в документах Microsoft Office : учебно-методическое пособие / М. Ф. Ванина. — Москва : Московский технический университет связи и информатики, 2018. — 58 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/92460.html

7. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

http://www.consultant.ru/ – Справочно-правовая система КонсультантПлюс
http://www.knigafund.ru/ – ЭБС «КнигаФонд»
http://www.cbr.ru/ – Официальный сайт ЦБ РФ
www.expert.ru – Официальный сайт журнала «Эксперт»
http://nacfin.ru/ – Национальное агентство финансовых исследований (НАФИ) раздел «Аналитика»
www.edu.ru – Российский образовательный портал
www.iet.ru – Институт экономики переходного периода
http://www.gks.ru – Официальный сайт Росстата

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Обучающиеся обеспечиваются дополнительным раздаточным материалом к лекционным и практическим занятиям в виде: методических рекомендаций к задачам и кейсам; макетов аналитических таблиц, графиков; схем алгоритмов управленческого процесса на предприятии; статей по анализу управленческих решений.

1. Лекционные занятия:

a) компьютерная аудитория (класс), оснащённая современными компьютерами с ОЗУ не менее 2 ГБ, жесткий диск не менее 200 ГБ, доступом в локальную корпоративную сеть МБИ и интернет,

b) презентационная техника (мультимедийный проектор или телевизионная панель с параметрами не ниже 720x576 пикселей/дюйм),

c) доска аудиторная для написания фломастером,

d) пакеты программного обеспечения (ПО) общего назначения (Системное программное обеспечение. Операционная система Microsoft Windows Professional,; Пакет офисных приложений Microsoft Office;Приложение для создания и просмотра электронных публикаций в формате PDF),

e) специализированное ПО для доступа к Единой электронной образовательной среде Института, специализированные программы для конкретных задач и кейсов.

2. Практические занятия:

a. рабочее место преподавателя (стол, стул), оснащенное компьютером с доступом в локальную корпоративную сеть МБИ и Интернет, подключенное к мультимедийному проектору или телевизионной панели, с установленным специальным программным обеспечением для доступа к Единой электронной образовательной среде Института.

b. доска аудиторная для написания фломастером,

c. рабочие места обучающихся (столы аудиторные, стулья аудиторные), оснащенные компьютерами с доступом в локальную корпоративную сеть МБИ и интернет, с установленным специальным программным обеспечением для доступа к Единой электронной образовательной среде Института.

Приложение 1

Методические указания к практическим занятиям

Цель выполнения практических заданий по дисциплине «Информационная безопасность» – приобретение практических навыков защиты информации.

Выполнение практических заданий требует от обучающегося предварительного изучения учебной и научной литературы и прочих информационных источников, в том числе периодических изданий и Интернет-ресурсов.

Перечень тем практических занятий представлен в нижеприведенной таблице.

Название темы учебной дисциплины	Перечень тем практических занятий
Постановка задачи обеспечения информационной безопасности	Методы и средства защиты информации
Основные понятия и определения в данной области	Методика оценки уровня информационной безопасности
Стандарты информационной безопасности	Функциональные возможности программы GNUPT
Обзор основных технологий защиты информационных систем	Основные характеристики МСЭ
Защита от вирусов	Сравнение российских VPN
Межсетевые экраны	ЭЦП на основе алгоритма Эль-Гамаля
Виртуальные частные сети	Алгоритмы Диффи-Хеллмана и Хилла
Основные методы криптографической защиты	Криптоанализ симметричных и асимметричных шифров.
Алгоритмы построения современных шифров с симметричными и асимметричными ключами	Алгоритмы шифрования.
Возможности применения методов криптографии для обеспечения безопасности электронных платежей	Криптоанализ хэш-функций

Требования к оформлению отчета по практической работе.

Отчет должен быть выполнен в машинописном варианте в соответствии с нормативными требованиями к оформлению научно-исследовательских отчетов. Рекомендуемый объем работы – 5-15 печатных листов. Способ оформления: 12-14 кегль, *Times New Roman*. Сдача – печатный вариант на листах формата А4 с одной стороны.

Отчет о выполнении самостоятельной работы представляется обучающимся в срок, строго соответствующий календарному графику учебного процесса данной дисциплины. В период экзаменационной сессии отчет на проверку не принимается.

При возврате проверенной, но не зачтенной работы обучающийся должен внести исправления в соответствии с замечаниями преподавателя и передать работу на повторную проверку. При отправке работы на повторную проверку обязательно представлять работу с указанными в первый раз замечаниями.

Отчеты, представленные без соблюдения указанных правил, на проверку не принимаются.

Приложение 2

Методические указания к самостоятельной работе обучающихся

Цель самостоятельной работы по дисциплине «Информационная безопасность» – закрепить теоретические знания и практические навыки в области защиты информации.

Самостоятельная работа предполагает изучение нормативных документов, теоретическую подготовку, написание эссе или реферата, подготовку к тестированию.

Перечень тем для самостоятельной работы представлен в нижеприведенной таблице.

Название темы учебной дисциплины	Перечень самостоятельной работы
Постановка задачи обеспечения информационной безопасности	Теоретическая подготовка, эссе
Основные понятия и определения в данной области	Теоретическая подготовка, эссе
Стандарты информационной безопасности	Теоретическая подготовка, эссе
Обзор основных технологий защиты информационных систем	Теоретическая подготовка, эссе
Защита от вирусов	Теоретическая подготовка, эссе
Межсетевые экраны	Теоретическая подготовка, эссе
Виртуальные частные сети	Теоретическая подготовка, эссе
Основные методы криптографической защиты	Теоретическая подготовка, эссе
Алгоритмы построения современных шифров с симметричными и асимметричными ключами	Теоретическая подготовка, эссе
Возможности применения методов криптографии для обеспечения безопасности электронных платежей	Теоретическая подготовка, эссе

Требования к оформлению отчета по самостоятельной работе

Отчет должен быть выполнен в машинописном варианте в соответствии с нормативными требованиями к оформлению научно-исследовательских отчетов. Рекомендуемый объем работы – 5-15 печатных листов. Способ оформления: 12-14 кегль, *Times New Roman*. Сдача – печатный вариант на листах формата А4 с одной стороны.

Отчет о выполнении самостоятельной работы представляется обучающимся в срок, строго соответствующий календарному графику учебного процесса данной дисциплины. В период экзаменационной сессии отчет на проверку не принимается.

При возврате проверенной, но не зачтенной работы обучающийся должен внести исправления в соответствии с замечаниями преподавателя и передать работу на повторную проверку. При отправке работы на повторную проверку обязательно представлять работу с указанными в первый раз замечаниями.

Отчеты, представленные без соблюдения указанных правил, на проверку не принимаются.

Темы эссе

Название темы дисциплины	Пример тем эссе
Постановка задачи обеспечения информационной безопасности	Компьютерная преступность в зарубежном законодательстве Компьютерная преступность в российском законодательстве Персональные данные и Интернет Защита баз данных
Основные понятия и определения в данной области	Международные стандарты информационной безопасности Российские стандарты информационной безопасности Политика информационной безопасности организации Обеспечение безопасности операционных систем
Стандарты информационной безопасности	Безопасность функционирования международной системы SWIFT Мошенничество в сети Интернет Промышленный шпионаж в сети Интернет Конкурентная разведка в сети Интернет Политика информационной безопасности организации Проблемы соблюдения авторских прав в сети Интернет Обеспечение правовой охраны компьютерных программ
Обзор основных технологий защиты информационных систем	Алгоритм организации секретной связи без опубликования ключей Итерационные блочные шифры Криптосхема Фейстеля Сертификация открытых ключей Сертификационный центр
Защита от вирусов	Применение расширенного алгоритма Евклида для расчета секретного ключа в алгоритме RSA Способы организации секретной связи
Межсетевые экраны	Безопасность облачных вычислений Биометрическая аутентификация пользователя Правовое регулирование электронного документооборота Персональные данные и Интернет Защита баз данных Защита информации в социальных сетях
Виртуальные частные сети	Режимы шифрования блочных шифров Режим CDC и его свойств Режим шифрования OFB и его свойства
Основные методы криптографической защиты	Пакет программ «Криптон-шифрование» Архивное шифрование и его реализация Криптология: основные понятия
Алгоритмы построения современных шифров с симметричными и асимметричными ключами	Сетевое шифрование и его реализация Виды атак на шифр
Возможности применения методов криптографии для обеспечения безопасности электронных платежей	Хэш-функция: назначение, требования, свойства Методы криптографии для обеспечения безопасности электронных платежей