Федеральное государственное бюджетное образовательное учреждение высшего образования

Московский государственный институт культуры

УТВЕРЖДЕНО
Председатель УМС
Библиотечно-информационного факультета
Боронина Н.В.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ (МОДУЛЯ)
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки/специальности (код, наименование) 09.03.02 Информационные системы и технологии

Профиль подготовки/специализация Информационные системы и цифровые технологии в культуре

Квалификация (степень) выпускника бакалавриат

Форма обучения очная

(РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели:
Ознакомление обучающихся с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей, и, конечно, методов их применения.

Задачи:
Сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния; передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации; сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Информационная безопасность и защита информации» входит в состав Блока 1 «Дисциплины (модули)» и относится к обязательной части /части, формируемой участниками образовательных отношений ОПОП по направлению подготовки 09.03.02 Информационные системы и технологии, профиль - Информационные системы и цифровые технологии в культуре.
Дисциплина «Информационная безопасность и защита информации» изучается в 3 семестре. Входные знания, умения и компетенции, необходимые для изучения данного курса, формируются в процессе изучения таких дисциплин, как: “Теоретические основы информатики”. В результате освоения дисциплины формируются знания, умения и навыки, необходимые для изучения следующих дисциплин и прохождения практик: “Информационная культура личности”, “Программирование”, “Проектирование ИС”, “Преддипломная практика” и других дисциплин.
Взаимосвязь курса с другими дисциплинами ООП способствует планомерному формированию необходимых компетенций и углубленной подготовке студентов к решению специальных практических профессиональных задач.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций *ОПК-3* в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки 09.03.02 Информационные системы и технологии

Перечень планируемых результатов обучения по дисциплине (модулю).

Компетенция (код и наименование)	**Индикаторы компетенций**	**Результаты обучения**
ОПК-3	ОПК-3.1.	Знает: основные требования информационной безопасности, правовые и

	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	этические нормы информационной деятельности, риски и уязвимости современной информационной среды, деструктивные возможности информационных технологий и цифрового контента, авторского права, прав интеллектуальной собственности, закономерности развития информационной сферы, понимает социальную ответственность информационного специалиста Умеет: применять информационно-коммуникационных технологии с учетом норм действующего законодательства, этических норма, требований информационной безопасности государства, организации, человека, противодействовать угрозам и упреждать риски воздействия на информационную среду Владеет: потребностью социально-ответственного поведения, навыками создания авторского контента и информационно-аналитических продуктов с учетом норм информационной и библиографической культуры, стремлением к сохранению культурного и научного наследия государства

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ *(модуля)*

4.1 Объем дисциплины (модуля)

Объем (общая трудоемкость) дисциплины «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ» составляет 3 зе, 108 акад. часов, из них контактных 34 акад.ч., СРС 21 акад.ч., формы контроля зачет, зачет с оценкой, экзамен

4.2. Структура дисциплины для очной формы обучения.

			Виды учебной работы*, включая самостоятельную работу студентов и трудоемкость (в часах)/ с указанием занятий, проводимых в интерактивных формах	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной

№ п/п	Тема/Раздел дисциплины		Лекции	Семинары/ Практич.	Конс	ИКР	СРС	аттестации *(по семестрам)*
Раздел I. Основы информационной безопасности								
1	**Понятие информационной безопасности. Основные составляющие**	*3*	*4*			*0*	*2*	*Экспресс-опрос по материалам лекции*
2	**Наиболее распространенные угрозы информационной безопасности и её составляющие**	*3*	*4*	*2*		*2*	*2*	*Семинар 1* *Тест к разделу 1*
Раздел II. Уровни информационной безопасности								
3	**Законодательный уровень информационной безопасности**	*3*	*4*	*2*		*0*	*0*	*Практическое занятие 2*
4	**Администра-тивный уровень информационной безопасности**	*3*	*4*	*2*		*2*	*0*	*Практическое занятие 3*
5	**Процедурный уровень информационной безопасности**	*3*	*2*	*2*		*0*	*5*	*Практическое занятие 4* *Тест к разделу 2*
Раздел III. Программно-технические меры по обеспечению информационной безопасности								
6	**Основные характеристики программно-технических мер**	*3*	*4*	*2*		*0*	*2*	*Практическое занятие 5*
7	**Идентификация и аутентификация**	*3*	*4*	*0*		*2*	*2*	*Экспресс-опрос на материал лекции*

8	**Протоколирование и аудит, шифрование, контроль целостности**	*3*	*2*	*2*		*0*	*4*	*Практическое занятие 6*
9	**Экранирование, анализ защищенности**	*3*	*4*	*2*		*2*	*2*	*Практическое занятие 7*
10	**Обеспечение высокой доступности**	*3*	*2*	*0*		*2*	*3*	*Тест к разделу 3*
	Итоговая форма контроля	*27*						*Экзамен*
	итого:		*34*	*16*		*10*	*21*	

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Текущий контроль выполнения заданий (контроль формирования компетенций) осуществляется регулярно, начиная с первой недели семестра (входящий контроль). Система текущего контроля успеваемости служит не только оценке уровня компетентностной подготовки обучающегося и способствует в дальнейшем наиболее качественному и объективному оцениванию его в ходе промежуточной аттестации, но и самооценке учащегося, стимулируя его усилия.

СИСТЕМА ОЦЕНИВАНИЯ

Форма контроля	**Компетенция**	**Оценка**
Текущий контроль: *- опрос* *-практическое занятие* *-тестирование*	*ОПК-3.1*	*зачтено/не зачтено* *зачтено / не зачтено (дифференциация определяется педагогом)* *зачтено /не зачтено (дифференциация определяется педагогом)*
Промежуточная аттестация *(экзамен)*	*ОПК-3.1*	*отлично/хорошо /удовлетворительно/неудовлетворительно*

КРИТЕРИИ ОЦЕНКИ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ

Оценка по дисциплине	**Критерии оценки результатов обучения по дисциплине**
«отлично»	Выставляется обучающемуся, если компетенция(ии), закрепленная за дисциплиной, сформирована (по индикаторам/ результатам обучения в формате знать-уметь-владеть) в полном объеме на уровне «высокий», и обучающийся демонстрирует как результат обучения следующие знания, умения и навыки: обучающийся глубоко и прочно усвоил теоретический и практический материал, продемонстрировал это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет сочетать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.
«хорошо»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне «хороший».
«удовлетворительно»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне «достаточный».

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

СЕМИНАРСКИЕ И ПРАКТИЧЕСКИЕ ЗАНЯТИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Тема: «Понятие информационной безопасности. Основные составляющие»

Семинар 1. Тема Основы информационной безопасности

Вопросы:

1. Вопросы информационной безопасности и правовое обеспечение защиты информации в нормативно-правовой базе России
2. Виды и источники угроз информационной безопасности
3. Компьютерные преступления : классификация, меры безопасности
4. Интернет-мошенничество : классификация, меры безопасности
5. Компьютерные вирусы и средства защиты от них.
6. Информационные войны и противодействие Интернет-терроризму

Практическое занятие 2. Тема: «Законодательный уровень информационной безопасности»

Тематика: изучение нормативно-правовых актов в сфере ИБ и их применение на практике.

Практические задания:

провести сравнительный анализ ФЗ-152 «О персональных данных» и ФЗ-149 «Об информации, информационных технологиях и о защите информации»;

выделить требования к защите персональных данных в соответствии с ФЗ-152 и сопоставить их с реальными процессами обработки данных в организации (на примере кейса);

изучить требования ФЗ-187 «О безопасности КИИ» и определить, относится ли гипотетическая организация к субъектам КИИ;

проработать сценарии нарушений законодательства в сфере ИБ (незаконный доступ к данным, неправомерное распространение информации) и определить меры ответственности;

выполнить задание: составить чек-лист соответствия информационной системы требованиям законодательства РФ.

Практическое занятие 3. Тема: «Административный уровень информационной безопасности»

Тематика: освоение методов организационного обеспечения ИБ.

Практические задания:
разработать политику информационной безопасности для организации (фрагмент документа с разделами: цели ИБ, область применения, роли и обязанности, меры защиты);
составить матрицу ролей и прав доступа для различных категорий сотрудников (руководство, ИТ-персонал, рядовые пользователи);
разработать регламент реагирования на инциденты ИБ (этапы: обнаружение, локализация, расследование, устранение последствий);
создать программу обучения сотрудников основам ИБ (темы, форматы, периодичность);
выполнить кейс: проанализировать инцидент ИБ и предложить меры административного характера для его предотвращения в будущем.

Практическое занятие 4. Тема: «Процедурный уровень информационной безопасности»
Тематика: отработка навыков создания и внедрения процедур обеспечения ИБ.
Практические задания:
разработать регламент работы с носителями информации (учёт, хранение, уничтожение);
составить инструкцию по резервному копированию данных с указанием RPO (Recovery Point Objective) и RTO (Recovery Time Objective);
создать процедуру обработки входящих электронных писем с потенциальными угрозами (фишинг, вредоносные вложения);
разработать чек-лист ежедневного контроля состояния ИБ для администратора;
выполнить практическое задание: на основе кейса (потеря данных из-за сбоя) предложить комплекс процедурных мер для минимизации рисков в будущем.

Практическое занятие 5. Тема: «Основные характеристики программно-технических мер»
Тематика: практическое освоение технических средств защиты информации.
Практические задания:
настроить антивирусную защиту на рабочей станции (выбор ПО, расписание проверок, обновление баз);
сконфигурировать межсетевой экран для сегмента сети (правила фильтрации трафика, блокировка подозрительных соединений);
развернуть систему обнаружения вторжений (IDS) и протестировать её на имитации атаки;
оценить эффективность защитных мер с помощью тестовых сценариев (попытка несанкционированного доступа, сканирование портов);
выполнить лабораторную работу: сравнить производительность системы при разных уровнях защиты (антивирус + firewall, антивирус + firewall + IDS).

Практическое занятие 6. Тема: «Протоколирование и аудит, шифрование, контроль целостности»
Тематика: применение методов мониторинга и криптографической защиты данных.
Практические задания:
настроить аудит доступа к файлам и папкам на ОС Windows/Linux (включение журналов событий, фильтрация записей);
проанализировать журнал событий на предмет подозрительной активности (неудачные попытки входа, изменение прав доступа);
зашифровать файл с помощью GPG/OpenSSL и передать его по незащищённому каналу;
проверить целостность данных с помощью хеш-функций (MD5, SHA−256) до и после передачи;
создать цифровую подпись для документа и проверить её валидность;
выполнить лабораторную работу: смоделировать сценарий утечки данных и продемонстрировать, как журналы аудита помогают выявить источник инцидента.

Практическое занятие 7. Тема: «Экранирование, анализ защищённости»
Тематика: освоение инструментов защиты периметра сети и оценки уровня безопасности.
Практические задания:

сконфигурировать правила фильтрации трафика на межсетевом экране (Firewall) для защиты веб-сервера;
провести сканирование сети на наличие уязвимостей с помощью Nmap/OpenVAS;
проанализировать результаты сканирования и классифицировать уязвимости по степени критичности (CVSS);
разработать план устранения выявленных уязвимостей (патчи, настройка параметров безопасности);
выполнить пентест базового уровня: имитировать атаку на веб-приложение и зафиксировать результаты;
составить отчёт по итогам анализа защищённости с рекомендациями по улучшению конфигурации сети и настроек безопасности.

КОНТРОЛЬНЫЕ ТЕСТЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ПО РАЗДЕЛАМ

Тестовые задания к разделу 1

1. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется
1. актуальностью информации
2. доступностью
3. качеством информации
4. целостностью

2. Согласно «Оранжевой книге» минимальную защиту имеет группа критериев
1. C
2. A
3. B
4. D

3. Организационные требования к системе защиты
1. управленческие и идентификационные
2. административные и аппаратурные
3. административные и процедурные
4. аппаратурные и физические

4. Основу политики безопасности составляет
1. программное обеспечение
2. управление риском
3. способ управления доступом
4. выбор каналов связи

5. Соответствие средств безопасности решаемым задачам характеризует
1. эффективность
2. корректность
3. адекватность
4. унификация

6. С точки зрения ФСТЭК основной задачей средств безопасности является обеспечение сохранности информации
1. защиты от НСД
2. простоты реализации

3. надежности функционирования

7. Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне
1. E5
2. E7
3. E4
4. E6

8. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это
1. аудит
2. аутентификация
3. авторизация
4. идентификация

9. Согласно «Оранжевой книге» уникальные идентификаторы должны иметь
1. наиболее важные субъекты
2. наиболее важные объекты
3. все субъекты
4. все объекты

10. Соответствие средств безопасности решаемым задачам характеризует
1. эффективность
2. корректность
3. адекватность
4. унификация

11. Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется
1. системой защиты
2. стандартом безопасности
3. профилем безопасности
4. профилем защиты

12. Для решения проблемы правильности выбора и надежности функционирования средств защиты в «европейских критериях» вводится понятие
1. унификации средств защиты
2. надежности защиты информации
3. адекватности средств защиты
4. оптимизации средств защиты

Тестовые задания к разделу 2
1. Организационные требования к системе защиты
1. управленческие и идентификационные
2. административные и аппаратурные
3. административные и процедурные
4. аппаратурные и физические

2. Основу политики безопасности составляет
1. программное обеспечение
2. управление риском

3. способ управления доступом
4. выбор каналов связи

3. Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности
1. Лендвера
2. С полным перекрытием
3. Белла-ЛаПадула
4. На основе анализа угроз

4. Из перечисленного услуга защиты целостности доступна на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом
1. 1, 2, 5
2. 1, 3, 5
3. 1, 2, 3
4. 4, 5, 6

5. Присвоение субъектам и объектам доступа уникального номера, шифра, ключа и
т.п. с целью получения доступа к информации — это
1. идентификация
2. аудит
3. авторизация
4. аутентификация

6. Из перечисленного типами услуг аутентификации являются:
1) идентификация;
2) достоверность происхождения данных;
3) достоверность объектов коммуникации;
4) причастность;
1. 3, 4
2. 1, 4
3. 2, 3
4. 1, 2

7. Как предотвращением неавторизованного использования ресурсов определена услуга защиты
1. аутентификация
2. причастность
3. контроль доступа
4. целостность

8. Пользовательское управление данными реализуется на уровне модели взаимодействия открытых систем
представления данных
1. канальном
2. сеансовом
3. прикладном

Тестовые задания к разделу 3
1. Наукой, изучающей математические методы защиты информации путем ее

преобразования, является
1. криптоанализ
2. криптология
3. стеганография
4. криптография

2. Конечное множество используемых для кодирования информации знаков называется
1. шифром
2. кодом
3. алфавитом
4. ключом

3. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет
1. криптология
2. стеганография
3. криптоанализ
4. криптография

4. Обеспечением скрытности информации в информационных массивах занимается
1. криптография
2. криптоанализ
3. криптология
4. стеганография

5. Два ключа используются в криптосистемах
1. с открытым ключом
2. с закрытым ключом
3. двойного шифрования
4. симметричных

6. Главным параметром криптосистемы является показатель
1. безошибочности шифрования
2. скорости шифрования
3. криптостойкости
4. надежности функционирования

7. Длина исходного ключа в ГОСТ 28147-89 (бит)
1. 128
2. 256
3. 64

8. Основной целью системы брандмауэра является управление доступом
1. к архивам
2. внутри защищаемой сети
3. к секретной информации
4. к защищаемой сети

9. Маршрутизаторы с фильтрацией пакетов осуществляют управление доступом методом проверки

адресов отправителя и получателя
1. содержания сообщений
2. электронной подписи
3. структуры данных

10. Из перечисленного система брандмауэра может быть: 1) репитором; 2) маршрутизатором; 3) ПК; 4) хостом; 5) ресивером
1. 3, 4, 5
2. 2, 3, 4
3. 1, 4, 5
4. 1, 2, 3

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПОДГОТОВКИ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
ВОПРОСЫ К ЭКЗАМЕНУ

1.Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб.
2.Доступность, целостность, конфиденциальность.
3.Компьютерное преступление, жизненный цикл информационных систем.
4.Сложные системы. Структурный подход.
5.Основные определения и критерии классификации угроз.
6.Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник.
7.Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.
8.Российское законодательство в области информационной безопасности.
9.Зарубежное законодательство в области информационной безопасности.
10.Стандарты и спецификации в области информационной безопасности.
11.Основные понятия, политика безопасности.
12.Жизненный цикл информационной системы.
13.Синхронизация программы безопасности с жизненным циклом систем. Управление рисками.
14.Основные классы мер процедурного уровня.
15.Управление персоналом. Физическая защита.
16.Поддержание работоспособности.
17.Реагирование на нарушения режима безопасности.
18.Планирование восстановительных работ.
19.Основные понятия программно-технического уровня. Архитектурная безопасность.
20.Экранирование. Анализ защищённости.
21.Отказоустойчивость. Безопасное восстановление.
22.Основные понятия криптографии.
24.Парольная аутентификация. Одноразовые пароли.
25.Идентификация/аутентификация с помощью биометрических данных.
26.Управление доступом. Ролевое управление доступом.
27.Активный аудит. Шифрование.
28.Симметричный метод шифрования.
29.Асимметричный метод шифрования.
30.Секретный и открытый ключ.
31.Криптография. Контроль целостности
32.Цифровые сертификаты.
33.Электронная цифровая подпись.

34.Экранирование. Фильтрация. Межсетевые экраны.
35.Классификация межсетевых экранов.
36.Архитектурная безопасность.
37.Транспортное экранирование. Анализ защищенности.
38.Сетевой сканер. Антивирусная защита.

ПРИМЕРЫ ПРАКТИЧЕСКИХ ЗАДАЧ НА ЭКЗАМЕНЕ

- проанализировать гипотетическую информационную систему организации и выделить объекты защиты (персональные данные, коммерческая тайна, финансовая отчётность и т.д.);
- для каждого объекта защиты определить требования по конфиденциальности (C), целостности (I) и доступности (A) в рамках модели CIA;
- составить таблицу с примерами угроз для каждого компонента модели CIA и возможными последствиями их реализации;
- разработать классификацию информации по уровням доступа (открытая, для служебного пользования, конфиденциальная, секретная);
- выполнить кейс-задание: на основе сценария инцидента (утечка данных) определить, какой компонент модели CIA был нарушен и какие меры могли бы предотвратить инцидент.

ПРИМЕРНЫЕ ТЕМЫ ДОКЛАДОВ (ПО ЖЕЛАНИЮ ОБУЧАЮЩЕГОСЯ)

1. Информационные ресурсы, подлежащие защите в сфере финансовой деятельности.
2. Классификация угроз информационной безопасности и их сравнительный анализ.
3. Информационная безопасность в современных условиях хозяйствования.
Общегосударственные цели, задачи и методы обеспечения информационной безопасности.
4. Понятия о видах вирусов. Классификация вирусов и угрозы для информационной инфраструктуры хозяйствующих субъектов.
5. Вида возможных нарушений информационной безопасности в сфере финансовой деятельности.
6. Отечественные и международные стандарты обеспечения информационной безопасности.
7. Особенности современной нормативно-правовой и методологической базы обеспечения информационной безопасности.
8. Основные нормативные руководящие документы, касающиеся конфиденциальной информации и государственной тайны, нормативно-справочные документы по обеспечению
информационной безопасности применяемые в финансовой деятельности.
9. Общие критерии оценки безопасности информационных систем и технологий ГОСТ 15408, как основа определения требований к обеспечению информационной безопасности.
10. Место информационной безопасности экономических систем в национальной безопасности страны.
11. Цели и задачи обеспечения национальной безопасности. Система целеполагания в структуре государственного и муниципального управления при обеспечении информационной безопасности.
12. Основные положения концепции информационной безопасности. Сравнительная таблица.
13. Государственные информационные ресурсы, подлежащие защите в сфере финансовой деятельности.
14. Взаимосвязь государственных и коммерческих информационных ресурсов

(конфиденциальной информации и государственной тайны).
15. Модели безопасности, и их применение.
16. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Оценка системы защиты информации.
17. Оценка эффективности средств и механизмов обеспечения информационной безопасности.
18. Методы анализа способов нарушений информационной безопасности.
19. Программно-аппаратные комплексы криптографической защиты, их характеристики и особенности применения. Сравнительная таблица.
20. Нормативно-правовая база криптографической защиты.
21. ЭЦП и особенности работы в системах государственного и муниципального управления.

ТЕСТ ПО ДИСЦИПЛИНЕ

Тест по информационной безопасности

Вариант 1

Часть 1. Закрытые вопросы (выберите один правильный ответ)

1. Что относится к основным свойствам информационной безопасности?
   а) доступность, целостность, конфиденциальность;
   б) масштабируемость, гибкость, модульность;
   в) скорость передачи, объём памяти, надёжность оборудования;
   г) стоимость, доступность, простота использования.
2. Что такое «окно опасности» в контексте информационной безопасности?
   а) период времени, когда система не защищена от конкретной угрозы;
   б) физический доступ к серверной комнате;
   в) интерфейс межсетевого экрана;
   г) окно программы для мониторинга угроз.
3. Какой метод шифрования использует один и тот же ключ для шифрования и расшифровки?
   а) асимметричный;
   б) симметричный;
   в) хеширование;
   г) квантовое шифрование.
4. Что является основной целью аутентификации?
   а) предоставление доступа ко всем ресурсам системы;
   б) подтверждение подлинности субъекта;
   в) шифрование данных;
   г) создание резервных копий.
5. Какой документ определяет правила и процедуры обеспечения информационной безопасности в организации?
   а) трудовой договор;
   б) политика безопасности;
   в) инструкция по эксплуатации оборудования;
   г) план эвакуации.

Часть 2. Открытые вопросы (дайте краткий ответ)

6. Дайте определение понятию «уязвимость» в информационной безопасности.
7. Перечислите три основных типа угроз доступности информации.
8. Кратко опишите принцип работы электронной цифровой подписи.
9. Назовите два российских закона, регулирующих вопросы информационной безопасности.

10. Что включает в себя понятие «управление рисками» в контексте информационной безопасности?

Вариант 2

Часть 1. Закрытые вопросы (выберите один правильный ответ)

1. Что понимается под «неприемлемым ущербом» в информационной безопасности?
   а) любые потери данных;
   б) ущерб, который превышает допустимый уровень для организации;
   в) технические сбои оборудования;
   г) потеря доступа к интернету.
2. Какой тип атаки направлен на нарушение доступности системы?
   а) фишинг;
   б) DDoS-атака;
   в) SQL-инъекция;
   г) социальная инженерия.
3. Что такое биометрическая аутентификация?
   а) использование пароля;
   б) использование физических характеристик пользователя (отпечаток пальца, голос и т.д.);
   в) использование смарт-карты;
   г) использование одноразового кода.
4. Какой компонент межсетевого экрана отвечает за фильтрацию трафика?
   а) антивирусный модуль;
   б) фильтр пакетов;
   в) модуль шифрования;
   г) система резервного копирования.
5. Что такое ролевое управление доступом?
   а) предоставление прав доступа на основе должности или функций пользователя;
   б) предоставление полного доступа всем пользователям;
   в) случайное распределение прав;
   г) доступ по паролю.

Часть 2. Открытые вопросы (дайте краткий ответ)

6. Объясните разницу между «угрозой» и «атакой» в информационной безопасности.
7. Перечислите три меры физической защиты информационных систем.
8. Кратко опишите принцип асимметричного шифрования.
9. Назовите два международных стандарта в области информационной безопасности.
10. Что подразумевается под «планированием восстановительных работ» после инцидента безопасности?

Ответы

Вариант 1

Закрытые вопросы: 1 — а, 2 — а, 3 — б, 4 — б, 5 — б.

Открытые вопросы:

6. Уязвимость — слабое место в системе, которое может быть использовано злоумышленником для проведения атаки.

7. DDoS-атаки, сбои оборудования, ошибки персонала.

8. Электронная цифровая подпись использует криптографические методы для подтверждения авторства и неизменности документа. Обычно включает хеш-функцию и асимметричное шифрование.

9. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон № 152-ФЗ «О персональных данных».

10. Управление рисками включает идентификацию, оценку, минимизацию и мониторинг рисков, связанных с информационной безопасностью.

Вариант 2

Закрытые вопросы: 1 — б, 2 — б, 3 — б, 4 — б, 5 — а.

Открытые вопросы:

6. Угроза — потенциальная возможность нарушения безопасности, атака — целенаправленное действие злоумышленника для реализации угрозы.

7. Контроль доступа в помещения, видеонаблюдение, защита от несанкционированного подключения оборудования.

8. Асимметричное шифрование использует пару ключей: открытый (для шифрования) и закрытый (для расшифровки).

9. ISO/IEC 27001, NIST SP 800-53.

10. Планирование восстановительных работ — разработка плана действий по восстановлению работоспособности систем и данных после инцидента, включая резервное копирование, порядок восстановления и ответственных лиц.