

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ярошенко Николай Николаевич

Должность: проректор по учебно-методической деятельности

Дата подписания: 04.06.2026 11:24:01

Уникальный программный ключ:

25cc77c6d2a242799b1569189212ec549db4bb3f

**Федеральное государственное бюджетное образовательное учреждение
высшего образования**

Московский государственный институт культуры

УТВЕРЖДЕНО

Председатель УМС

**Библиотечно-информационного
факультета**

Боронина Н.В.

**РАБОЧАЯ ПРОГРАММА 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
<i>ОПК-3</i>	ОПК-3.1.	Знает: основные требования информационной безопасности, правовые и

	<p>Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p>	<p>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</p> <p>Умеет: применять информационно-коммуникационные технологии с учетом норм действующего законодательства, этических норма, требований информационной безопасности государства, организации, человека, противодействовать угрозам и упреждать риски воздействия на информационную среду</p> <p>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</p>
--	--	--

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.

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

№ 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	<i>Экспресс-опрос по материалам лекции</i>
2	Наиболее распространенные угрозы информационной безопасности и её составляющие	3	4	2		2	2	<i>Семинар 1 Тест к разделу 1</i>
Раздел II. Уровни информационной безопасности								
3	Законодательный уровень информационной безопасности	3	4	2		0	0	<i>Практическое занятие 2</i>
4	Администра- тивный уровень информационной безопасности	3	4	2		2	0	<i>Практическое занятие 3</i>
5	Процедурный уровень информационной безопасности	3	2	2		0	5	<i>Практическое занятие 4 Тест к разделу 2</i>
Раздел III. Программно-технические меры по обеспечению информационной безопасности								
6	Основные характеристики программно- технических мер	3	4	2		0	2	<i>Практическое занятие 5</i>
7	Идентификация и аутентификация	3	4	0		2	2	<i>Экспресс-опрос на материал лекции</i>

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

4.3. Содержание разделов дисциплины (модуля)

№	Наименование раздела (подраздела, темы) дисциплины	Содержание
1	Понятие информационной безопасности. Основные составляющие	Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем.
2	Наиболее распространенные угрозы информационной безопасности и её составляющие	Основные определения и критерии классификации угроз. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности*
3	Законодательный уровень информационной безопасности	Российское законодательство в области информационной безопасности. Стандарты и спецификации в области информационной безопасности.
4	Административный уровень информационной безопасности	Основные понятия, политика безопасности. Жизненный цикл информационной системы. Синхронизация программы безопасности с

		жизненным циклом систем. Управление рисками.
5	Процедурный уровень информационной безопасности	Основные классы мер процедурного уровня. Управление персоналом. Физическая защита*. Поддержание работоспособности. Реагирование на нарушения режима безопасности*. Планирование восстановительных работ.
6	Основные характеристики программно-технических мер	Основные понятия программно-технического уровня. Архитектурная безопасность. Экранирование. Анализ защищённости. Отказоустойчивость*. Безопасное восстановление.
7	Идентификация и Аутентификация	Основные понятия. Парольная аутентификация. Одноразовые пароли. Идентификация/аутентификация с помощью биометрических данных*. Управление доступом. Ролевое управление доступом.
8	Протоколирование и аудит, шифрование, контроль целостности	Основные понятия. Активный аудит. Шифрование*. Симметричный метод шифрования. Асимметричный метод шифрования. Секретный и открытый ключ. Криптография. Контроль целостности*. Цифровые сертификаты. Электронная цифровая подпись.
9	Экранирование, анализ Защищенности	Основные понятия. Экранирование. Фильтрация. Межсетевые экраны. Классификация межсетевых экранов. Архитектурная безопасность*. Транспортное экранирование. Анализ защищенности. База данных уязвимостей. Сетевой сканер*. Антивирусная защита.
10	Обеспечение высокой Доступности	Эффективность услуг. Время недоступности. Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Обеспечение обслуживаемости. Туннелирование.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4

1.	<i>Понятие информационной безопасности. Основные составляющие</i>	<i>Лекция 1.</i>	<i>Вводная лекция с использованием видеоматериалов</i> <i>Экспресс-опрос</i>
2	<i>Наиболее распространенные угрозы информационной безопасности и её составляющие</i>	<i>Лекция 2. Семинар 1</i>	<i>Проблемная лекция Семинар 1</i>
3	<i>Законодательный уровень информационной безопасности</i>	<i>Лекция 3. Практическое занятие 2.</i>	<i>Лекция-дискуссия</i> <i>Обсуждение выступлений на практическом занятии</i>
4	<i>Административный уровень информационной безопасности</i>	<i>Лекция 4. Практическое занятие 3.</i>	<i>Лекция с разбором конкретной ситуации</i> <i>Дискуссия на практическом занятии</i>
5	<i>Процедурный уровень информационной безопасности</i>	<i>Лекция 5. Практическое занятие 4.</i>	<i>Лекция с применением техники обратной связи</i> <i>Практическое занятие - развернутая беседа с обсуждением работ</i>
6	<i>Основные характеристики программно-технических мер</i>	<i>Лекция 6. Практическое занятие 5.</i>	<i>Лекция-дискуссия</i> <i>Дискуссия на практическом Занятии</i>
7	<i>Идентификация и аутентификация</i>	<i>Лекция 7.</i>	<i>Проблемная лекция</i> <i>Экспресс-опрос по материалам лекции</i>
8	<i>Протоколирование и аудит, шифрование, контроль целостности</i>	<i>Лекция 8. Практическое занятие 6.</i>	<i>Лекция с применением техники обратной связи</i> <i>Дискуссия на практическом Занятии</i>

9	Экранирование, анализ защищенности	Лекция 9. Практическое занятие 7.	Проблемная лекция
10	Обеспечение высокой доступности	Лекция 10.	Лекция - визуализация Пробное тестирование

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

Литература

1. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: <http://www.iprbookshop.ru/77319.html>

2. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учеб. пособие / Ю.Н. Сычев. — М. : ИНФРА-М, 2019. — 223 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cc15bb22f5345.11209330. - Режим доступа: <http://znanium.com/catalog/product/979415>

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.

6. 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). Контроль и оценивание выполнения осуществляется на 2 неделе семестра. 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.

6.1. 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

6.2. Критерии оценки результатов по дисциплине

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
«отлично»	<p>Выставляется обучающемуся, если компетенция(ии), закреплённая за дисциплиной, сформирована (по индикаторам/ результатам обучения в формате знать-уметь-владеть) в полном объёме 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.</p> <p>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.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p>
«хорошо»	<p>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.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне «хороший».</p>
«удовлетворительно»	<p>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.</p> <p>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.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне «достаточный».</p>
«неудовлетворительно»/ не зачтено	<p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые</p>

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
	<p>ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>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.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

6.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

КОНТРОЛЬНЫЕ ТЕСТЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ПО РАЗДЕЛАМ

Тестовые задания к разделу 1

1. Совокупность свойств, обуславливающих 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. С
2. А
3. В
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 аппаратные
3. административные и процедурные
4. аппаратные 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 отчетность и т.д.);
- для каждого объекта защиты определить требования по конфиденциальности (С), целостности (I) и доступности (А) 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. Виды 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 межсетевое 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.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Список литературы и источников

Основная:

1. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 с. — ISBN 978-5-4487-0147-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/72341.html>

2. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 с. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/86357.html>

3. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш [и др.]. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 242 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/62945.html>

4. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учеб. пособие / Ю.Н. Сычев. — М. : ИНФРА-М, 2019. — 223 с. — (Высшее образование: Бакалавриат). —
www.dx.doi.org/10.12737/textbook_5cc15bb22f5345.11209330. —Режим доступа:
<http://znanium.com/catalog/product/979415>

5. Фаронов, А. Е. Основы информационной безопасности при работе на

компьютере / А. Е. Фаронов. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: <http://www.iprbookshop.ru/52160.html>.

6. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: <http://www.iprbookshop.ru/77319.html>.

Дополнительная:

7. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 236 с.: - Режим доступа: <http://znanium.com/catalog/product/987215>

8. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 с. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/86938.html> . — Режим доступа: для авторизир. пользователей

9. Фомин, Д. В. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем / составители И. Л. Боброва, К. А. Севрук. — М. : Московский технический университет связи и информатики, 2015. — 35 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: <http://www.iprbookshop.ru/61737.html>.

7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

- Библиографические записи электронных ресурсов составляется в соответствии с требованиями ГОСТ 7.0.100-2018 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления».

Культура РФ: <https://www.culture.ru/> [Электронный ресурс]: сайт (дата обращения 19.12.25)

Доступ в ЭБС:

ООО «Электронное издательство ЮРАЙТ».

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Методические рекомендации по самостоятельной работе студентов

Самостоятельная работа обучающихся включает в себя такие виды и формы как: подготовка к практическому занятию, конспектирование литературы по изучаемой теме и др. Для более углубленного изучения материала задание для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий для самостоятельной работы, по возможности, следует ориентироваться на наглядное представление материала

Семинар 1. Тема Основы информационной безопасности

ТЕМА: 1.1. Понятие информационной безопасности. Основные составляющие.
В рамках поведения занятия предусмотрено освоение следующих компетенций:
ОПК-3 - способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Рекомендовано проработать следующие вопросы:

1. Понятие «Информационная безопасность».
2. Место информационной безопасности и Информационной безопасности РФ.
3. Обеспечение информационной безопасности.
4. Обеспечение доступности информации.
5. Обеспечение целостности информации.
6. Обеспечение конфиденциальности информации.

Литература

1. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: <http://www.iprbookshop.ru/77319.html>

ТЕМА 1.2. Наиболее распространенные угрозы информационной безопасности и ее составляющие

Рекомендовано проработать следующие вопросы

1. Перечислите виды угроз безопасности информации.
2. Каковы источники угроз безопасности информации?
3. Каковы проблемы защиты электронной информации?
4. Что такое компьютерное преступление?
5. Дайте классификацию компьютерным преступлениям.
6. Правовое обеспечение защиты информации.
7. Опишите механизмы преступлений с использованием пластиковых карт.
8. Опишите мошенничество на Интернет-аукционах.
9. Компьютерные вирусы и средства защиты от них.
10. Троянские программы, использование троянских программ для совершения компьютерных преступлений.
11. Что такое информационная атака?
12. Что такое информационная война?
13. Что такое электронный терроризм?

Литература

1. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учеб. пособие / Ю.Н. Сычев. — М. : ИНФРА-М, 2019. — 223 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cc15bb22f5345.11209330. - Режим доступа: <http://znanium.com/catalog/product/979415>

Подготовка к практическому занятию 2. ТЕМА. Уровни информационной безопасности

ТЕМА: 2.1. Тема. Законодательный уровень информационной безопасности.

В рамках поведения лабораторного занятия предусмотрено освоение следующих компетенций:

ОПК-3 - способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-

коммуникационных технологий и с учетом основных требований информационной безопасности

Рекомендуется самостоятельно проработать вопросы

1. Задачи Информационной безопасности общества.
2. Законодательно-правовой уровень обеспечения информационной безопасности
3. Ответственность за нарушение в сфере информационной безопасности
4. Стандарты информационной безопасности

Литература:

1. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: <http://www.iprbookshop.ru/77319.html>

2. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учеб. пособие / Ю.Н. Сычев. — М. : ИНФРА-М, 2019. — 223 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cc15bb22f5345.11209330. - Режим доступа: <http://znanium.com/catalog/product/979415>

Подготовка к практическому занятию 3.

Рекомендуется самостоятельно проработать следующие вопросы:

1. Цели, задачи и содержание административного уровня.
2. Политика информационной безопасности
3. Содержание политики информационной безопасности фирмы
4. Разработка политики информационной безопасности

Литература:

1. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: <http://www.iprbookshop.ru/77319.html>

Подготовка к практическому занятию 4.

Рекомендуется самостоятельно проработать следующие вопросы:

1. Управление персоналом
2. Поддержание работоспособности
3. Планирование восстановительных работ
4. Физическая защита
5. Реагирование на нарушение безопасного режима

Литература:

1. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: <http://www.iprbookshop.ru/77319.html>

Подготовка к практическому занятию 4. Тема Основные характеристики программно-технических мер обеспечения информационной безопасности

Рекомендуется самостоятельно проработать следующие вопросы:

1. Основные понятия программно-технического уровня информационной безопасности
2. Объективные причины, затрудняющие обеспечение надежной защиты
3. Основные сервисы безопасности

Литература

1. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: <http://www.iprbookshop.ru/77319.html>

Подготовка к практическому занятию 5.

Рекомендуется самостоятельно проработать следующие вопросы:

1. Понятие идентификация/аутентификация
2. Причины возможного снижения надежности идентификации
3. Парольная аутентификация
4. Проблемы парольной аутентификации
5. Характеристики идентификации/аутентификации с помощью биометрических данных
6. Каким угрозам подвержена биометрическая аутентификация

Литература

1. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: <http://www.iprbookshop.ru/77319.html>.

Подготовка к практическому занятию 3.

Рекомендуется самостоятельно проработать следующие вопросы:

В рамках поведения лабораторного занятия предусмотрено освоение следующих компетенций:

ОПК-3 способностью участвовать в управлении проектом, программой внедрения технологических и продуктовых инноваций или программой организационных изменений

Вопросы

1. Протоколирование и аудит. Основные понятия.
2. Активный аудит. Основные понятия.
3. Функциональные компоненты и архитектура.
4. Шифрование.
5. Контроль целостности.

Литература

1. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: <http://www.iprbookshop.ru/77319.html>

Практическое занятие 5. Тема Экранирование, анализ защищенности

В рамках поведения лабораторного занятия предусмотрено освоение следующих компетенций:

ОПК-3- способностью участвовать в управлении проектом, программой внедрения технологических и продуктовых инноваций или программой организационных изменений

Вопросы

1. Понятие межсетевого экранирования
2. Типы межсетевых экранов, краткая характеристика.
3. Технология виртуальных частных сетей (VPN).

Литература

1. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: <http://www.iprbookshop.ru/77319.html>

Практическое занятие 6. Тема Обеспечение высокой доступности

В рамках поведения лабораторного занятия предусмотрено освоение следующих компетенций:

ОПК-3 - способностью участвовать в управлении проектом, программой внедрения технологических и продуктовых инноваций или программой организационных изменений

Вопросы

1. Основные понятия:
 - заданный уровень доступности
 - Эффективности
 - Время недоступности
2. Основные меры обеспечения высокой доступности
 - Структуризация системы
 - Высокая отказоустойчивость (резервирование, тиражирование);
 - Обслуживаемость информационной системы.

Литература

1. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: <http://www.iprbookshop.ru/77319.html>.

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.

При изучении дисциплины обучающимися используются следующие информационные технологии:

- аудиовизуальное представление обучающимся с помощью компьютера содержания отдельных тем дисциплины на лекционных занятиях;
- предоставление обучающимся доступа к учебному плану, рабочей программе дисциплины в электронной форме, к электронно-библиотечной системе института, содержащей учебно-методические материалы по дисциплине в электронной форме, к информационным справочным системам, которые используется при осуществлении образовательного процесса по дисциплине, посредством электронной информационно-образовательной среды института из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет»;
- фиксация хода образовательного процесса по дисциплине посредством электронной информационно-образовательной среды института;
- формирование электронного портфолио обучающегося по дисциплине посредством электронной информационно-образовательной среды института.

При осуществлении образовательного процесса по дисциплине используется следующее лицензионное программное обеспечение:

Word, Excel, Power Point;

Adobe Photoshop;

Adobe Premiere;

Power DVD;

Media Player Classic.

10. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины требует наличия лекционного кабинета со следующим оборудованием:

1. Ноутбук с программным обеспечением Microsoft PowerPoint;

2. Проектор для демонстрации слайдов Microsoft PowerPoint;

3. Экран для демонстрации слайдов Microsoft PowerPoint.

Для преподавания дисциплины необходим доступ к электронной информационно-образовательной среде (ЭИОС) филиала, электронному каталогу библиотеки института, а

также оборудование для мультимедийных презентаций.

Освоение дисциплины предполагает использование академической аудитории для проведения лекционных и практических занятий с необходимыми техническими средствами

(оборудование для мультимедийных презентаций).

11. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов (при наличии)

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
 - обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
 - письменные задания оформляются увеличенным шрифтом;
 - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
 - в форме аудиофайла.
- для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа;
 - в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
 - устройством для сканирования и чтения с камерой SARA CE;
 - дисплеем Брайля PAC Mate 20;
 - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
 - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
 - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - передвижными, регулируемые эргономическими партами СИ-1;
 - компьютерной техникой со специальным программным обеспечением.

Составитель(и):

*Доктор технических наук, профессор кафедры библиотечно-информационных наук
В.М.Тютюнник*

АННОТАЦИЯ ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

код и наименование подготовки
09.03.02 Информационные системы и технологии

профиль/специализация
Информационные системы и цифровые технологии в культуре

Цель дисциплины (*модуля*):

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

Дисциплина (*модуль*) направлена на формирование следующих компетенций:

- ОПК-3.1. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

В результате освоения дисциплины (*модуля*) обучающийся должен:

Знать: основные требования информационной безопасности, правовые и 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

Уметь: применять информационно-коммуникационные технологии с учетом норм действующего законодательства, этических норма, требований информационной безопасности государства, организации, человека, противодействовать угрозам и упреждать риски воздействия на информационную среду

Владеть: 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

По дисциплине (модулю) предусмотрена промежуточная аттестация в форме *зачета/зачёта с оценкой/экзамена*.

Общая трудоемкость освоения дисциплины (модуля) составляет 3 зачетных единицы.