ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНА

Решением Ученого совета
АНО ВО «Центральный университет»
«07» марта 2024 г.
Протокол №1

Рабочая программа дисциплины (модуля)
«Информационная безопасность»

Направление подготовки: *02.03.01 Математика и компьютерные науки*

Направленность (профиль) подготовки: *Искусственный интеллект*

Квалификация (степень) выпускника: *бакалавр*

Форма обучения: *очная*

Срок освоения программы: *4 года*

Год набора: *2024*

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0215B0C000D1B3FEB44A37EE631E0C27D4
Владелец: Ивашкевич Евгений Васильевич
Действителен: с 13.01.2026 до 13.04.2027

Электронный документ

Москва
2024

Содержание

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Информационная безопасность» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по специальности 02.03.01 Математика и компьютерные науки, профиль Искусственный интеллект, утвержденный приказом Министерства науки и высшего образования Российской Федерации № 807 от 23.08.2017 года.

Изучение дисциплины (модуля) «Информационная безопасность» позволяет защитить информационные ресурсы и данные от несанкционированного доступа, предотвращая угрозы и кибератаки. Это обеспечивает сохранность конфиденциальности, целостности и доступности информации, что критично для стабильной работы организаций и безопасности пользователей.

Дисциплина (модуль) «Информационная безопасность» разработана и утверждена совместно с АО «Лаборатория Касперского».

Место дисциплины (модуля) в структуре образовательной программы

Настоящая дисциплина (модуль) включена в учебные планы по программам подготовки бакалавриата по направлению 02.03.01 Математика и компьютерные науки, профиль Искусственный интеллект и входит в часть Блока 1, формируемую участниками образовательных отношений, как дисциплина по выбору.

Дисциплина (модуль) изучается на 2, 3 ил 4 курсе в 4, 5, 6, 7 или 8 семестре на выбор.

Цель изучения дисциплины (модуля): формирование знаний и навыков по защите информации и информационных систем от различных угроз и несанкционированного доступа.

Задачи изучения дисциплины (модуля) направлены на формирование у студентов следующий знаний, умений и навыков:

- знание основных угроз информационной безопасности;
- знание стратегий защиты информации;
- знание нормативных документов, регламентирующих защиту информации;
- умение формировать требования по защите информации;
- умение вести учет затрат и рисков при выработке стратегий защиты информации;
- навык проведения аудита безопасности информационных систем;
- навык составления оптимального плана комплекса мер по защите информации.

2. Перечень планируемых результатов обучения

Компетенции, формируемые в результате освоения дисциплины (модуля) при проведении учебных занятий в форме контактной работы обучающихся с педагогическими работниками Университета и в форме самостоятельной работы обучающихся:

Компетенция	Содержание компетенции	Индикатор компетенции	Перечень планируемых результатов обучения по дисциплине (модулю)
УК-1.	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1.	Знает методы поиска и анализа информации в области искусственного интеллекта, основные принципы критической оценки источников информации и их релевантности
		УК-1.2.	Умеет критически оценивать источники информации и синтезировать данные из различных источников для решения задач, применять системный подход к анализу и решению комплексных проблем
		УК-1.3.	Имеет практический опыт работы с современными инструментами и технологиями для обработки информации, формулировании и структурировании задач на основе полученной информации
ОПК-1.	Способен консультировать и использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в профессиональной деятельности	ОПК-1.1.	Знает основные концепции и теории в области математического анализа и смежных дисциплин; методы и подходы, используемые в различных областях математики
		ОПК-1.2.	Умеет применять математические методы для решения профессиональных задач
		ОПК-1.3.	Имеет практический опыт разработки и реализация математических моделей в профессиональной деятельности
ОПК-6	Способен разрабатывать алгоритмы и компьютерные программы, пригодные	ОПК-6.1.	Знает алгоритмы разработки, компьютерные программы, а также алгоритмы вычислительной математики в области

	для практического применения		искусственного интеллекта
		ОПК-6.2.	Умеет разрабатывать математические программные продукты и комплексы с использованием современных технологий программирования в области искусственного интеллекта
		ОПК-6.3.	Имеет практический опыт разработки интеллектуальных информационных систем для визуализации результатов исследований в области искусственного интеллекта
ПК-1.	Способен формулировать задачи с математической точностью, обосновывать утверждения строго и анализировать полученные результаты в области математики и компьютерных наук	ПК-1.1.	Знает методы и подходы к формулированию задач, а также основные принципы математического доказательства и анализа результатов
		ПК-1.2.	Умеет корректно ставить и формулировать математические задачи, применять строгие методы доказательства и анализировать полученные результаты
		ПК-1.3.	Имеет опыт работы с задачами в области математики и компьютерных наук, включая применение математических методов для решения практических задач

3. Тематический план

№п/п	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы				ТКУ (текущий контроль успеваемости)
		Очная форма				
		Контактная работа		Контроль	Самостоятельная работа	
		Лекции	Семинары (практические занятия)			
1	Основы безопасности корпоративной инфраструктуры	6	6		24	Домашние задания
2	Вредоносное программное обеспечение	6	6		26	Домашние задания
3	Криптографическая защита информация	6	6		26	Домашние задания
4	Методы защиты информации	6	6		26	Домашние задания
5	Аудит безопасности информационных систем	6	6		26	Домашние задания Коллоквиум
	Зачет с оценкой			2		
	Итого:	***30***	***30***	***2***	***128***	
Объем дисциплины (модуля) (в ак. ч.)		***190***				
Объем дисциплины (модуля) (в зач. ед.)		***5***				

4. Содержание дисциплины (модуля)

№п/п	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам
1	Основы безопасности корпоративной инфраструктуры	Администрирование ОС: Windows, Linux Сети передачи данных. Модель OSI Виртуализация и контейнеры
2	Вредоносное программное обеспечение	Классификация вредоносного программного обеспечения. Социальная инженерия и фишинг. Анализ вредоносных программ (реверс-инжиниринг).
3	Криптографическая защита информация	Основы криптографической защиты информации. Управление доступом: идентификация, аутентификация, авторизация. Управление ключами и PKI
4	Методы защиты информации	Классификация программных средств защиты информации. Мониторинг и реагирование на инциденты (цифровая криминалистика). Риск-ориентированный подход при построении системы защиты. Планирование финансовых ресурсов.
5	Аудит безопасности информационных систем	Нормативные основы защиты информации в РФ. Модель угроз и злоумышленника. Тестирование на проникновение - методология и программный инструментарий. Безопасность приложений

5. Учебно-методическое обеспечение

Университет располагает полным набором лицензионного и свободно распространяемого программного обеспечения, включая продукты отечественного производства.

Каждый студент в течение всего периода обучения получает индивидуальный неограниченный доступ к электронно-библиотечной системе и электронной информационно-образовательной среде университета. Эти системы предоставляют возможность доступа к ресурсам из любой точки, где есть подключение к сети Интернет, как на территории университета, так и за его пределами.

Студентам обеспечен удаленный доступ к современным профессиональным базам данных и информационным справочным системам.

Основная литература:

1. Родичев, Ю. А. Информационная безопасность. Национальные стандарты Российской Федерации : учебное пособие / Ю. А. Родичев. - 3-е изд. - Санкт-Петербург : Питер, 2023. - 384 с. - (Серия «Учебник для вузов»). - ISBN 978-5-4461-2112-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/2123368.

2. Скабцов, Н. Аудит безопасности информационных систем : практическое руководство / Н. Скабцов. - Санкт-Петербург : Питер, 2018. - 272 с. - (Серия «Библиотека программиста»). - ISBN 978-5-4461-0662-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1760857.

3. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. - 2-е изд. - Москва : ДМК Пресс, 2023. - 594 с. - ISBN 978-5-89818-506-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/2107178.

4. Скляров, Д. В. Искусство защиты и взлома информации : практическое руководство / Д. В. Скляров. - Санкт-Петербург : БХВ-Петербург, 2004. - 289 с. - ISBN 5-94157-331-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1856816.

5. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567915.

6. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567672.

Дополнительная литература:

7. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2025. — 154 с. — (Высшее образование). — ISBN 978-5-534-17866-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581502.

8. Козырь, Н. С. Оценка рисков и аудит информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2025. — 186 с. — (Высшее образование). — ISBN 978-5-534-17864-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581501.

6. Материально-техническое обеспечение

Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех

видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Изучение дисциплины (модуля) обеспечивается в учебных аудиториях, оснащенных:

— столами и стульями;
— компьютерной техникой;
— механическими калькуляторами;
— специализированным оборудованием, включая демонстрационное оборудование.

Помещения для самостоятельной работы обучающихся, в том числе приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

Обучающимся предоставляется доступ (в том числе удаленный) к ресурсам информационно-телекоммуникационной сети «Интернет», электронным ресурсам (в том числе электронным библиотечным системам, современным профессиональным базам данных и информационным справочным системам):

№	Наименование портала (издания, курса, документа)	Ссылка
1.	Научная электронная библиотека elibrary.ru библиотека	https://elibrary.ru/defaultx.asp
2.	База данных для IT-специалистов	https://habr.com
3.	База данных ScienceDirect	https://www.sciencedirect.com
4.	Официальный сайт Министерства науки и высшего образования Российской Федерации	https://minobrnauki.gov.ru/
5.	Федеральный портал «Российское образование"	https://www.edu.ru/
6.	Информационная система "Единое окно доступа к образовательным ресурсам"	http://window.edu.ru/
7.	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru/
8.	Федеральный центр информационно - образовательных ресурсов	http://fcior.edu.ru/

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), в том числе комплект лицензионного программного обеспечения, современные профессиональные базы данных и информационные справочные системы:

Наименование ПО	Производство	Лицензионное / свободно распространяемое
Операционные системы:		
Microsoft Imagine (Windows Client, Server)	зарубежное	лицензионное
Браузеры:		
Яндекс.Браузер	отечественное	свободно распространяемое
Google Chrome	зарубежное	свободно распространяемое
Офисные приложения:		

Microsoft Imagine (Visio, OneNote)	зарубежное	лицензионное
TeXstudio	зарубежное	свободно распространяемое
Adobe Acrobat Reader	зарубежное	свободно распространяемое
Программное обеспечение для планирования и учета времени:		
Toggle app	зарубежное	свободно распространяемое
Системы управления проектами:		
Microsoft Imagine (Project)	зарубежное	лицензионное
Системы управления базами данных:		
Microsoft Imagine (SQL Server)	зарубежное	лицензионное
Системы резервного копирования (backup):		
Acronis Backup Advanced for HyperV	зарубежное	лицензионное
Справочно-правовые системы:		
КонсультантПлюс: справочно-правовая система	отечественное	лицензионное
Средства антивирусной защиты:		
Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition	отечественное	лицензионное
Среды разработки:		
Visual Studio Code	зарубежное	свободно распространяемое
Bash (Unix shell)	зарубежное	свободно распространяемое
Anaconda	зарубежное	свободно распространяемое
Robotic Operating System	зарубежное	свободно распространяемое
CopelliaSim	зарубежное	свободно распространяемое
Google Colaboratory	зарубежное	свободно распространяемое
Пакеты программных средств и библиотек:		
AutoPsy	зарубежное	свободно распространяемое
Interactive Disassembler (IDA)	зарубежное	свободно распространяемое
Системы управления библиографической информацией:		
Zotero	зарубежное	свободно распространяемое
Сервисы и службы:		
Bind	зарубежное	свободно распространяемое
Docker	зарубежное	свободно распространяемое

7. Методические и оценочные материалы

Методические указания для обучающихся по освоению дисциплины (модуля)

В процессе изучения дисциплины (модуля) «Информационная безопасность» в рамках текущего контроля успеваемости используются такие виды учебной работы, как лекции, семинары, коллоквиумы, домашние задания, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков профессиональной лексики, закрепление практических профессиональных компетенций, поощрение инициатив.

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект лекций: кратко и схематично фиксировать основные идеи, выводы и обобщения лекции; выделять важные мысли, ключевые слова и термины. Необходимо отметить вопросы или материалы, которые вызывают затруднения, и попытаться найти ответы в рекомендованной литературе. Если разобраться в материале не удается, следует сформулировать вопрос и задать его преподавателю на консультации или во время семинарского (практического) занятия.

Участие в семинаре (аудиторная работа) – активная работа студента на семинаре,

его ответы на вопросы преподавателя и участие в дискуссии.

Для успешного участия в семинаре студентам рекомендуется заранее ознакомиться с темой обсуждения, прочитать необходимые материалы и подготовить вопросы. Важно активно слушать и вовлекаться в дискуссию, высказывая свои мнения и аргументируя их. При ответах на вопросы преподавателя стоит быть уверенным, четким и логичным, опираясь на изученный материал. Также полезно поддерживать диалог с однокурсниками, чтобы обогатить обсуждение и расширить свои знания.

Домашнее задание – набор задач по темам недели.

При работе над домашними заданиями важно внимательно ознакомиться с требованиями и сроками выполнения. Рекомендуется разбивать задания на этапы, чтобы избежать перегрузки и лучше усвоить материал. Использовать различные источники информации, включая учебники и онлайн-ресурсы, для более глубокого понимания темы.

Коллоквиум – устные ответы на вопросы, список которых известен студенту заранее.

В процессе подготовки к коллоквиуму необходимо проанализировать учебные материалы, ознакомившись с лекциями, учебниками и дополнительными источниками, акцентируя внимание на ключевых темах. Рекомендуется создать структурированные конспекты, выделяя основные идеи, термины и формулы.

Самостоятельная работа – работа студентов, направленная на углубленное изучение отдельных тем и вопросов учебной дисциплины (модуля).

В процессе самостоятельной работы студенты взаимодействуют с рекомендованными материалами при минимальном участии преподавателя. Задачи студента включают работу с конспектами лекций (обработка текста), повторное изучение учебных материалов, планов и тезисов ответов, изучение дополнительных тем, выполнение учебно-исследовательских заданий и другое.

Система оценивания результатов обучения по дисциплине (модулю)

Критерии получения уровня и оценивания сформированности компетенций по дисциплине (модулю) «Информационная безопасность»

Оценивание уровня учебных достижений, обучающихся по дисциплине (модулю), осуществляется в виде текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация по дисциплине (модулю) осуществляется в форме ***зачета с оценкой***, при этом проводится оценка компетенций, сформированных по дисциплине. Для оценивания текущего контроля успеваемости и промежуточной аттестации используется десятибалльная шкала оценивания, которая соотносится с традиционной пятибалльной шкалой следующим образом:

Десятибалльная оценка	**Пятибалльная оценка**	**Оценка за зачет**	**Общая характеристика результата обучения по дисциплине (модулю)**
10	Отлично	Зачтено	Студент полностью владеет знаниями, изложенными в рабочей программе, и глубоко осмысляет дисциплину. Он самостоятельно и логически последовательно отвечает на все вопросы, акцентируя внимание на наиболее важном. Умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать
9	Отлично	Зачтено	
8	Отлично	Зачтено	

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
			изученный материал, выделяя ключевые моменты и устанавливая причинно-следственные связи. Четко формулирует ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты дисциплины (модуля) с практическими задачами.
7	Хорошо	Зачтено	Студент обладает знаниями предмета почти в полном объеме рабочей программы и самостоятельно, логически последовательно и всесторонне отвечает на все вопросы, акцентируя внимание на наиболее значимых моментах. Он умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя его ключевые аспекты и устанавливая причинно-следственные связи. Формулирует свои ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные ситуационные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты предмета с практическими задачами.
6	Хорошо	Зачтено	
5	Удовлетворительно	Зачтено	Студент обладает базовыми знаниями по дисциплине (модулю), но испытывает трудности при самостоятельных ответах и использует неточные формулировки. В ходе ответов он допускает ошибки, касающиеся сути вопросов. Студент способен решать только самые простые задачи и владеет лишь минимальным набором методов исследования.
4	Удовлетворительно	Зачтено	
3	Не сдан	Не зачтено	Студент не овладел обязательным минимумом знаний по предмету и не может ответить на вопросы, даже если преподаватель задает дополнительные наводящие вопросы.
2	Не сдан	Не зачтено	
1	Не сдан	Не зачтено	

Дисциплина (модуль) «Информационная безопасность» оценивается следующим образом:

Активность	Вес	Количество	Описание
Домашние задания	50%	15	Набор задач по темам недели
Коллоквиум	25%	5	Письменная работа с набором задач, которые нужно решить за ограниченное время
Зачет с оценкой	25%	1	Письменная или устная работа над заданием, направленным на проверку полученных знаний и навыков по дисциплине (модулю)

Формула расчёта итоговой оценки по дисциплине (модулю) «Информационная безопасность»: «0,5 × среднее за домашние задания + 0,25 × среднее за коллоквиум + 0,25 × зачет с оценкой».

Текущий контроль успеваемости обучающихся по дисциплине (модулю)

Примерные домашние задания

Домашнее задание по теме «Последствия атак. Обнаружение и удаление»

1. Проанализируйте реальный случай кибератаки (например, WannaCry или NotPetya) и опишите её последствия для организации.
2. Составьте алгоритм действий по обнаружению и удалению вредоносного ПО на компьютере.
3. Исследуйте современные инструменты для обнаружения вредоносного ПО и сделайте сравнительную таблицу их возможностей.
4. Опишите основные признаки заражения системы вредоносным ПО.
5. Разработайте план восстановления информационной системы после успешной атаки.

Домашнее задание по теме «Методы социальной инженерии»

1. Подготовьте доклад о пяти наиболее распространённых методах социальной инженерии с примерами.
2. Составьте сценарий фишингового письма и объясните, как распознать его признаки.
3. Проанализируйте реальные случаи успешных атак с использованием социальной инженерии и выделите ошибки жертв.
4. Разработайте рекомендации для сотрудников по предотвращению атак социальной инженерии.
5. Проведите ролевую игру: один студент выступает в роли злоумышленника, другой — потенциальной жертвы, и проанализируйте результаты.

Домашнее задание

Что используем

- Java Spring
- Spring Security
- Keycloak (с PostgreSQL DB)
- Docker + Compose

Что надо сделать

1. Реализовать простое веб-приложение с использованием Java Spring. Тематика – на ваш вкус. Требований к контенту, хранению в БД и т.д. нет. Что должно быть
   a. Главная страница (лендинг), доступный без авторизации всем (а-ля у нас классный сервис, регистрируйтесь)
   b. Страница регистрации и логина (можно брать стандартную из Keycloak, можете свою красивую форму для нее сделать)
   c. Страница, которая доступна любому зарегистрированному пользователю (а-ля личный кабинет, данные какие-то по клиенту и т.д.)
   d. Страница, которая должна быть доступна только администратору (а-ля какая-то админка)
2. Подключить Spring Security и подружить это с Keycloak. Настроить авторизацию и аутентификацию, настроить роли “user” и “admin”
3. Запаковать приложение в docker compose. Главное требование – при проверке должно быть достаточно сделать docker compose up и все должно работать
4. Показать клиентский путь и продемонстрировать со скриншотами в README регистрацию, вход, назначение ему в Keycloak роли администратора (и как меняется веб-приложение при этом действии для него)
5. В вашем приложении должна быть настроена защита от CSRF
6. В вашем приложении должны быть настроены CORS Policy
7. Сделайте так, чтобы в ваше приложение можно было попадать только через NGINX. Рекомендую делать по DNS записям так: «example.com» – ваше приложение, а «api.example.com» – ваше API для него. Добавить такие записи при отсутствии DNS сервера можно через /etc/hosts в UNIX-like системах
8. Настройте на NGINX базовый MTLS. Выпустите свой CA для клиентов и настройте его так, чтобы если к вам обращались без сертификата, то получали бы ошибку 403 (работающий пример - https://smallstep.com/hello-mtls/doc/server/nginx)
9. При помощи переменной `$ssl_client_s_dn` отразите в NGINX логах `log_format` DN сертификата.
10. Выпустите клиентский сертификат, установите в систему CA для доверия и клиентский сертификат. Продемонстрируйте, что при работе с браузером не возникает ошибок самоподписанного сертификата. Проверьте, что в логи NGINX попала запись о ваших похождениях

Как предоставить результаты

- Репозиторий с кодом сервиса на Git
- В репозитории ОБЯЗАТЕЛЬНО должен быть отчет. В отчете ОБЯЗАТЕЛЬНО должны быть картинки с демонстрацией функциональности

Примерные вопросы для подготовки к семинарам

Вопросы к семинару по теме «Контроль доступа. Мониторинг данных»

1. Какие основные модели контроля доступа существуют и в чем их отличия (например, DAC, MAC, RBAC)?
2. Какие методы аутентификации и авторизации применяются для обеспечения контроля доступа?
3. Каковы основные задачи и методы мониторинга данных в корпоративной сети?
4. Какие инструменты и технологии используются для обнаружения несанкционированного доступа?
5. Каковы основные принципы построения политики контроля доступа и мониторинга для защиты информации?

Примерные вопросы для коллоквиума

Коллоквиум по теме «Вредоносное программное обеспечение»

1. Перечислите и кратко охарактеризуйте основные виды вредоносного программного обеспечения.
2. Опишите распространённые методы заражения компьютеров вредоносным ПО.
3. Проанализируйте последствия атаки типа ransomware для организации.
4. Какие признаки указывают на заражение системы вирусом?
5. Опишите основные этапы процесса обнаружения и удаления вредоносных программ.
6. Какие существуют методы защиты от вирусов на уровне пользователя?
7. Расскажите о роли антивирусного ПО и его основных функциях.
8. Приведите пример реальной атаки с использованием вредоносного ПО и опишите её последствия.
9. Объясните, как работает эвристический анализ в антивирусных программах.
10. Разработайте алгоритм действий при подозрении на заражение компьютера вредоносным ПО.

Коллоквиум по теме «Криптографическая защита информация»

1. Объясните разницу между симметричным и асимметричным шифрованием.
2. Назовите и кратко охарактеризуйте основные алгоритмы симметричного шифрования.
3. Расскажите о принципах работы алгоритма RSA.
4. Что такое цифровая подпись и как она обеспечивает целостность и аутентичность данных?
5. Опишите процесс аутентификации пользователей с использованием криптографических методов.
6. Какие существуют методы управления криптографическими ключами?
7. Приведите пример применения цифровых сертификатов в инфраструктуре открытых ключей (PKI).
8. Объясните, как работает алгоритм хеширования и его роль в информационной безопасности.
9. Опишите угрозы, связанные с неправильным управлением ключами.
10. Разработайте схему обмена зашифрованными сообщениями между двумя пользователями с использованием асимметричного шифрования.

Коллоквиум по теме «Тестирование на проникновение и аудит безопасности»

1. Опишите основные этапы проведения тестирования на проникновение.
2. В чем различия между внешним и внутренним пентестингом?
3. Какие инструменты используются для сканирования уязвимостей? Приведите примеры.
4. Как проводится анализ уязвимостей и оценка их критичности?

5. Расскажите о методах эксплуатации уязвимостей в рамках пентестинга.
6. Какие требования предъявляются к отчету по результатам тестирования на проникновение?
7. Приведите примеры рекомендаций по устранению обнаруженных уязвимостей.
8. Как обеспечивается соответствие требованиям стандартов безопасности (например, ISO 27001) в ходе аудита?
9. Опишите роль автоматизированных и ручных методов в пентестинге.
10. Разработайте план проведения аудита безопасности для малой организации.

Задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ	Компетенция
1.	Какой вид вредоносного ПО способен самостоятельно распространяться и заражать другие файлы и системы? A) Троян B) Вирус C) Руткит D) Бэкдор	B	УК-1
2.	Какой метод социальной инженерии основан на использовании чувства срочности и страха для получения доступа к информации? A) Спуфинг B) Вишинг C) Фишинг D) Сниффинг	C	УК-1
3.	Какой математический алгоритм используется для асимметричного шифрования данных? A) AES B) DES C) MD5 D) RSA	D	ОПК-1
4.	Как называется процесс проверки подлинности пользователя с помощью криптографических методов? A) Авторизация B) Аутентификация C) Шифрование D) Хэширование	B	ПК-1
5.	Какая технология позволяет контролировать и блокировать передачу конфиденциальных данных за пределы организации? A) VPN B) Firewall C) IDS D) DLP (Data Loss Prevention)	D	ПК-1
6.	Как называется политика, регулирующая права доступа пользователей к информационным ресурсам? A) Контроль доступа B) Шифрование C) Аутентификация D) Логирование	A	УК-1

7.	Какой метод тестирования безопасности включает моделирование атак злоумышленников для выявления уязвимостей? A) Пентестинг B) Фаззинг C) Ревизия кода D) Мониторинг	A	УК-1
8.	Как называется инструмент для автоматизированного анализа уязвимостей в сетях и системах? A) Wireshark B) Metasploit C) Nessus D) Nmap	C	ОПК-6
9.	Как называется вредоносное ПО, которое маскируется под полезное приложение?	Троян	ОПК-6
10.	Как называется метод социальной инженерии, при котором злоумышленник звонит жертве для получения конфиденциальной информации?	Вишинг	ОПК-1
11.	Как называется цифровой код, подтверждающий подлинность сообщения?	Цифровая подпись	ПК-1
12.	Назовите процесс мониторинга и анализа трафика для обнаружения подозрительной активности.	Мониторинг данных	УК-1