ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНА

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

Рабочая программа дисциплины (модуля) «Информационная безопасность»

Направление подготовки: *02.04.01 Математика и компьютерные науки*

Направленность (профиль) подготовки: *Backend-разработка*

Квалификация (степень) выпускника: *магистр*

Форма обучения: *очная*

Срок освоения программы: *2 года*

Год набора: *2024*

Москва
2024

Электронный документ

Содержание

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Информационная безопасность» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – магистратура по специальности 02.04.01 Математика и компьютерные науки, профиль Backend-разработка, утвержденный приказом Министерства науки и высшего образования Российской Федерации № 810 от 23.08.2017 года.

Изучение дисциплины (модуля) «Информационная безопасность» дает знания в области информационной безопасности становятся критически важными для защиты личной и корпоративной информации. Кроме того, осознание принципов информационной безопасности способствует созданию безопасной цифровой среды, что является необходимым условием для устойчивого развития бизнеса и общества в целом.

Место дисциплины (модуля) в структуре образовательной программы

Настоящая дисциплина (модуль) включена в учебный план по программе подготовки магистратуры по направлению 02.04.01 Математика и компьютерные науки, профиль Backend-разработка и входит в вариативную часть Блока 1, формируемую участниками образовательных отношений.

Дисциплина (модуль) изучается на 2 курсе в 3 семестре.

Цель изучения дисциплины (модуля): формирование у студентов знаний и навыков, необходимых для защиты информации и информационных систем от угроз, рисков и атак.

Задачи изучения дисциплины (модуля):

— формирование знаний основных принципов и методов обеспечения информационной безопасности программных систем;

— формирование знаний современных криптографических алгоритмов и их применение в разработке;

— формирование знаний распространённыя типов уязвимостей и угроз для веб-приложений и системного уровня;

— формирование умения применять криптографические механизмы (шифрование, хеширование, цифровая подпись) в программных решениях;

— формирование умения обнаруживать и анализировать типовые уязвимости в веб-приложениях и системах;

— формирование умения использовать инструменты для оценки безопасности и тестирования приложений;

— формирование навыка разрабатывать программное обеспечение с учётом требований безопасности;

— формирование навыка формулировать и реализовывать базовые меры защиты информации на уровне приложения и системы;

— формирование навыка оценивать риски, связанные с реализацией функциональности, и делать выбор в пользу безопасных решений.

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-6.	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1.	Знает основные методы самооценки и анализа своей деятельности, а также принципы управления временем и целеполагания
		УК-6.2	Умеет ставить реалистичные и достижимые цели, определять приоритеты в своей деятельности, а также разрабатывать и внедрять планы по совершенствованию своих навыков и компетенций на основе полученной самооценки
		УК-6.3	Имеет практический опыт применения методов самооценки в своей профессиональной деятельности, включая участие в тренингах, семинарах и проектах, направленных на развитие личной эффективности и профессионального роста
ОПК-2.	Способен создавать и исследовать новые математические модели в естественных науках, совершенствовать и разрабатывать концепции, теории и методы	ОПК-2.1.	Знает основные математические модели и методы, используемые в естественных науках, включая статистическое моделирование, дифференциальные уравнения и численные методы, а также современные подходы к исследованию и анализу данных
		ОПК-2.2	Умеет разрабатывать и адаптировать математические модели для решения конкретных проблем в естественных науках, проводить их анализ и верификацию, а также интерпретировать полученные результаты в контексте научных исследований
		ОПК-2.3	Имеет практический опыт создания и исследования математических моделей в рамках научных проектов или исследований, включая участие в публикациях, конференциях или коллаборациях, где были разработаны и апробированы новые концепции и методы

ПК-3.	Способен решать задачи профессиональной деятельности, формулировать результат, увидеть следствия полученного результата	ПК-3.1.	Знает основные принципы и методы решения задач профессиональной деятельности, а также способы формулирования и представления результатов, включая анализ последствий и их значимость в контексте проекта
		ПК-3.2.	Умеет применять математические и компьютерные методы для решения конкретных задач, формулировать четкие и обоснованные результаты, а также анализировать их последствия для дальнейших действий и решений
		ПК-3.3.	Имеет практический опыт в решении профессиональных задач, включая участие в проектах, где были получены результаты и проанализированы их следствия, что способствовало принятию обоснованных решений
ПК-4.	Способен публично представлять собственные и известные научные результаты	ПК-4.1.	Знает основные принципы эффективного публичного выступления, методы визуализации данных и основные требования к научным презентациям, включая структуру и содержание
		ПК-4.2.	Умеет четко и логично формулировать свои научные результаты, адаптируя их для различных аудиторий, а также использовать визуальные средства для улучшения восприятия информации
		ПК-4.3.	Имеет практический опыт участия в научных конференциях, семинарах или других мероприятиях, где успешно представлял свои и известные научные результаты, получая обратную связь и взаимодействуя с аудиторией

3. Тематический план

№ п/п	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы				ТКУ (текущий контроль успеваемости)
		Очная форма				
		Аудиторная работа		Контроль	Самостоятельная работа	
		Лекции	Семинары (практические занятия)			
1	Основные криптографические алгоритмы	3	3		20	Домашнее задание Подготовка к семинару
2	Безопасность на уровне операционной системы	4	4		20	Домашнее задание Подготовка к семинару
3	Безопасность веб-приложений	4	4		20	Домашнее задание Тест
4	Организационные аспекты информационной безопасности	4	4		20	Домашнее задание Подготовка к семинару
	Зачет с оценкой			4		
Итого:		***15***	***15***	***4***	***80***	
Объем дисциплины (модуля) (в ак. ч.)		***114***				
Объем дисциплины (модуля) (в зач. ед.)		***3***				

4. Содержание дисциплины (модуля)

№п/п	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам
1	Основные криптографические алгоритмы	Симметричное шифрование (AES, DES) Асимметричное шифрование (RSA, Эллиптические кривые) Хэш-функции и цифровые подписи Протоколы обмена ключами (Диффи-Хеллман)
2	Безопасность на уровне операционной системы	Управление правами доступа и аутентификация Механизмы контроля целостности и защиты памяти Обнаружение и предотвращение вредоносного ПО Журналирование и аудит безопасности
3	Безопасность веб-приложений	Аутентификация и управление сессиями Защита от атак типа XSS, CSRF и SQL-инъекций Шифрование данных и HTTPS Безопасность API и веб-сервисов
4	Организационные аспекты информационной безопасности	Политики и стандарты безопасности Оценка рисков и управление инцидентами Обучение персонала и повышение осведомленности Соответствие нормативным требованиям и аудит

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. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/569267.

Дополнительная литература:

1. Компьютерные сети : учебник и практикум для вузов / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва : Издательство Юрайт, 2025. — 515 с. — (Высшее образование). — ISBN 978-5-534-21452-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/572239.

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;

— 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 к 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
Распределенные системы:		
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, тесты, 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.

Тест – особая форма проверки знаний. Проводится после освоения одной или нескольких тем и свидетельствует о качестве понимания основных понятий изучаемого материала. Тестовые задания составлены к ключевым понятиям, основным разделам, важным терминологическим категориям изучаемой дисциплины (модуля).

Для подготовки к тесту необходимо знать терминологический аппарат дисциплины (модуля), понимать смысл научных категорий и уметь их использовать в профессиональной лексике. Владение понятийным аппаратом, включённым в тестовые задания, позволяет преподавателю быстро проверить уровень понимания студентами важных методологических категорий.

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 (модуль). Он самостоятельно и логически последовательно отвечает на все вопросы, акцентируя внимание на наиболее важном. Умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать 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.
9	Отлично	Зачтено	
8	Отлично	Зачтено	
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
6	Хорошо	Зачтено	

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
			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.
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	Описание
Домашние задания	50%	За каждое из заданий можно набрать 10 баллов
Аудиторная работа	10%	На каждом семинаре студент может заработать баллы за интересные вопросы, работу на семинаре и выполнение заданий
Тесты	10%	Ответы на вопросы по изученным темам
Зачет с оценкой	30%	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 + 0,1 × среднее за аудиторную работу +0,1 × среднее за тесты+ 0,3 × зачет с оценкой».

Текущий контроль успеваемости обучающихся по дисциплине (модулю)
Примерные вопросы для подготовки к семинарам

1. Принципы симметричного шифрования: алгоритмы AES и DES
2. История и особенности алгоритма DES
3. Современные стандарты симметричного шифрования: AES
4. Асимметричное шифрование: основы и применение RSA
5. Криптография на эллиптических кривых: принципы и преимущества
6. Сравнение RSA и криптографии на эллиптических кривых
7. Хэш-функции: назначение и свойства
8. Популярные хэш-алгоритмы: MD5, SHA-1, SHA-256
9. Цифровые подписи: концепция и использование
10. Протокол Диффи-Хеллмана: обмен ключами в небезопасной среде
11. Управление правами доступа в операционных системах
12. Механизмы аутентификации пользователей
13. Контроль целостности данных и защита памяти ОС
14. Методы обнаружения вредоносного программного обеспечения
15. Средства предотвращения и удаления вредоносного ПО
16. Журналирование событий безопасности в ОС
17. Аудит безопасности и его роль в защите систем
18. Основы аутентификации и управление сессиями в веб-приложениях
19. Защита веб-приложений от XSS-атак: методы и инструменты
20. Механизмы предотвращения CSRF-атак
21. SQL-инъекции: выявление и защита
22. Использование HTTPS для защиты данных в вебе
23. Сертификаты SSL/TLS и их роль в безопасности веб-приложений
24. Безопасность REST API: аутентификация и авторизация
25. Угрозы и методы защиты веб-сервисов
26. Практические аспекты реализации криптографии в приложениях
27. Анализ уязвимостей операционных систем
28. Современные тренды в борьбе с вредоносным ПО
29. Инструменты и методы аудита безопасности веб-приложений
30. Комплексный подход к обеспечению безопасности веб-приложений и ОС

Примерные домашние задания

Домашнее задание: Безопасность на уровне операционной системы — Управление правами доступа и аутентификация

1. Опишите основные модели управления доступом (DAC, MAC, RBAC) и приведите примеры их применения.
2. Настройте права доступа для файлов и папок в выбранной ОС (Windows или Linux) и опишите результат.
3. Исследуйте и опишите методы аутентификации пользователей, используемые в вашей операционной системе.
4. Создайте сценарий настройки двухфакторной аутентификации для учетной записи пользователя.

5. Проанализируйте риски, связанные с использованием слабых паролей, и предложите рекомендации по их усилению.

Домашнее задание: Безопасность на уровне операционной системы — Контроль целостности, защита памяти, обнаружение и предотвращение вредоносного ПО, журналирование и аудит

1. Изучите и опишите методы контроля целостности файлов в ОС (например, использование хэш-сумм).
2. Объясните, как механизмы защиты памяти (ASLR, DEP) помогают предотвратить атаки.
3. Проведите исследование популярных антивирусных программ и опишите принципы их работы.
4. Настройте и проанализируйте системные журналы безопасности в вашей ОС.
5. Опишите процесс проведения аудита безопасности и его значение для организации.

Домашнее задание: Безопасность веб-приложений — Аутентификация, управление сессиями, защита от атак, шифрование и безопасность API

1. Реализуйте простую форму аутентификации с управлением сессиями на примере веб-приложения.
2. Опишите основные методы защиты от XSS и CSRF атак и приведите примеры кода.
3. Проведите анализ уязвимости веб-страницы к SQL-инъекциям и предложите способы защиты.
4. Объясните роль HTTPS и SSL/TLS в защите данных при передаче по сети.
5. Исследуйте методы аутентификации и авторизации в API и опишите лучшие практики их реализации.

Примерные задания для тестов

Тест по теме: Аутентификация и управление сессиями, защита от XSS, CSRF и SQL-инъекций, шифрование данных и HTTPS, безопасность API и веб-сервисов

1. Что из перечисленного является примером многофакторной аутентификации?
   а) Пароль
   б) Отпечаток пальца + пароль
   в) Имя пользователя
   г) Электронная почта

2. Какой механизм обычно используется для управления состоянием пользователя в веб-приложениях?
   а) Cookies
   б) DNS
   в) FTP
   г) SMTP

3. Что такое XSS-атака?
   а) Внедрение вредоносного SQL-кода
   б) Внедрение вредоносного скрипта в веб-страницу
   в) Перехват сессии пользователя
   г) Подмена DNS-записей

4. Какой из методов наиболее эффективен для защиты от CSRF-атак?
   а) Использование HTTPS

б) Валидация пользовательского ввода
в) Использование токенов (CSRF-токенов)
г) Ограничение длины пароля

5. Что такое SQL-инъекция?
   а) Внедрение вредоносного SQL-кода через вводимые данные
   б) Атака на протокол HTTPS
   в) Перехват сессии пользователя
   г) Использование слабого пароля

6. Какой протокол обеспечивает защищённое соединение между клиентом и сервером?
   а) HTTP
   б) FTP
   в) HTTPS
   г) SMTP

7. Что такое SSL/TLS?
   а) Протоколы для передачи электронной почты
   б) Протоколы шифрования данных в интернете
   в) Языки программирования
   г) Типы баз данных

8. Какой из способов наиболее эффективно защищает API от несанкционированного доступа?
   а) Использование открытых ключей
   б) Аутентификация и авторизация с помощью токенов (например, OAuth)
   в) Использование HTTP вместо HTTPS
   г) Открытый доступ без ограничений

9. Что из перечисленного является примером уязвимости, связанной с управлением сессиями?
   а) Слабый пароль
   б) Перехват сессионного идентификатора (Session Hijacking)
   в) Использование HTTPS
   г) Ограничение доступа по IP

10. Какой метод помогает предотвратить XSS-атаки при отображении пользовательских данных?
    а) Валидация и экранирование вывода
    б) Использование длинных паролей
    в) Частая смена пароля
    г) Использование токенов CSRF

11. Что происходит при атаке CSRF?
    а) Злоумышленник подделывает запросы от имени пользователя
    б) Внедряется вредоносный SQL-код
    в) Перехватывается сессионный идентификатор
    г) Используется слабое шифрование

12. Какой из способов передачи данных наиболее безопасен?
    а) Передача по HTTP
    б) Передача по HTTPS

в) Передача по FTP
г) Передача по Telnet

13. Что такое OAuth в контексте безопасности API?
    а) Протокол для обмена сообщениями
    б) Протокол авторизации, позволяющий предоставлять ограниченный доступ
    в) Вид шифрования
    г) Тип базы данных

14. Какой из методов помогает защитить веб-приложение от SQL-инъекций?
    а) Использование параметризованных запросов (prepared statements)
    б) Использование простых текстовых паролей
    в) Отключение HTTPS
    г) Использование cookies без защиты

15. Что из перечисленного НЕ относится к методам защиты сессий?
    а) Установка флага HttpOnly для cookie
    б) Использование токенов CSRF
    в) Хранение пароля в сессии в открытом виде
    г) Ограничение времени жизни сессии

Задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ	Компетенция
1.	Какой из перечисленных алгоритмов относится к симметричному шифрованию? а) RSA б) AES в) Диффи-Хеллман г) Эллиптические кривые	б	ОПК-2
2.	Что из перечисленного является основным механизмом контроля целостности в ОС? а) Журналирование б) Аутентификация в) Контроль доступа на основе ролей (RBAC) г) Хэш-функции	а	ПК-3
3.	Какой метод наиболее эффективен для защиты веб-приложения от CSRF-атак? а) Использование HTTPS б) Внедрение токенов CSRF в) Использование сложных паролей г) Ограничение доступа по IP	б	ПК-4
4.	Назовите алгоритм асимметричного шифрования, основанный на свойствах эллиптических кривых.	Эллиптические кривые (ECC)	ОПК-2
5.	Как называется протокол, позволяющий двум сторонам безопасно обмениваться ключами через незащищённый канал?	Диффи-Хеллман	ПК-3
6.	Какой элемент безопасности ОС отвечает за проверку личности пользователя?	Аутентификация	УК-6
7.	Как называется процесс управления временем жизни пользователя в веб-приложении после входа в систему?	Управление сессиями	ПК-3

8.	Как называется документ, регламентирующий требования и правила по информационной безопасности в организации?	Политика безопасности	УК-6