ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНА

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

Рабочая программа дисциплины (модуля) «Введение в информационную 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)** 3
2. **Перечень планируемых результатов обучения** 5
3. **Тематический план** 7
4. **Содержание дисциплины (модуля)** 7
5. **Учебно-методическое обеспечение** 8
6. **Материально-техническое обеспечение** 8
7. **Методические и оценочные материалы** 10

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Введение в информационную безопасность» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению 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) «Введение в информационную 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.

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 вариативную часть Блока 1, формируемую участниками образовательных отношений.

Дисциплина (модуль) является выборной и доступна для изучения на 3 курсе в 5 семестре после успешного освоения дисциплины (модуля): «Основы промышленной разработки».

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

Задачи изучения дисциплины (модуля):

— изучить основные понятия, угрозы и принципы информационной безопасности, включая модели защиты и стандарты;

— практические методы и технологии защиты информации, таких как шифрование, аутентификация и контроль доступа;

— научиться анализировать законодательные и этические аспектов информационной безопасности, а также развитие умений по выявлению и предотвращению киберугроз.

В результате освоения дисциплины (модуля) обучающийся должен:

знать:

— основные понятия информационной безопасности и триаду CIA;

— правовые и экономические основы защиты информации: 152-ФЗ, GDPR, оценка стоимости инцидента, ROI;

— классификацию атак на пользователя и принципы базовой защиты: фишинг, вредоносное ПО, аутентификация, управление секретами;

— основные понятия криптографии и границы применимости криптографических механизмов;

— принципы сетевой и периметровой безопасности;

— угрозы безопасности систем искусственного интеллекта и использование генеративного ИИ в качестве инструмента атаки;

уметь:

— применять понятийный аппарат информационной безопасности при описании систем и сценариев угроз;

— проводить базовый правовой аудит проекта на соответствие требованиям 152-ФЗ и GDPR;

— настраивать базовые средства персональной защиты: многофакторную аутентификацию, менеджер паролей, управление секретами в проекте;

— применять криптографические инструменты и анализировать TLS-сертификаты;

— анализировать сетевой трафик и распознавать атаки Человек посередине;

— Распознавать атаки на ИИ-системы и признаки синтетического медиаконтента;

владеть:

— методикой построения модели угроз и анализа инцидентов по CIA, STRIDE, MITRE ATT&CK;

— методикой формирования бизнес-обоснования инвестиций в информационную безопасность;

— навыками применения базовых защитных механизмов: аутентификации, управления секретами, шифрования;

— навыками анализа сетевого трафика и оценки периметра безопасности;

— навыками распознавания атак на системы искусственного интеллекта и синтетического медиаконтента.

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 разработки, 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 для практического применения	ОПК-6.1.	Знает алгоритмы разработки, компьютерные программы, а также алгоритмы вычислительной математики в области 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.	Обладает базовыми знаниями, полученными в области математических наук, программирования и информационных технологий
		ПК-1.2.	Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в математике и информатике
		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				
		Аудиторная работа		Контроль	Самостоятельная работа	
		Лекции	Семинары (практические занятия)			
1	Понятийный аппарат, методология и контекст	8	6	2	26	Аудиторная работа Контрольная работа
2	Атаки на пользователя и базовая защита	8	8	4	26	Аудиторная работа Коллоквиум
3	Инструменты криптографии	2	2		26	Аудиторная работа
4	Периметр безопасности	2	2		26	Аудиторная работа
5	Прикладные системы и безопасность ИИ	8	8		24	Аудиторная работа
	Зачет с оценкой			2		
	Итого:	***28***	***26***	***8***	***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	Понятийный аппарат, методология и контекст	Основные понятия информационной безопасности Риск-ориентированный подход, моделирование угроз Жизненный цикл атаки и процессы реагирования на инциденты Правовые основы защиты информации
2	Атаки на пользователя и базовая защита	Социальная инженерия и фишинговые атаки Вредоносное программное обеспечение Аутентификация, авторизация, идентификация Управление секретами и доступами в проекте
3	Инструменты криптографии	Инструменты криптографии
4	Периметр безопасности	Периметр безопасности: сетевые атаки
5	Прикладные системы и безопасность ИИ	Цифровая криминалистика и разборы инцидентов Безопасность веб-сервисов Безопасность систем искусственного интеллекта Дезинформация, дипфейки и верификация источников

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. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588741.

2. Родичев, Ю. А. Информационная безопасность: нормативно-правовые аспекты : учебное пособие / Ю. А. Родичев. - Санкт-Петербург : Питер, 2021. - 272 с. - ISBN 978-5-4461-9992-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1857033.

Дополнительная литература:

3. Райтман, М. А. Информационная безопасность для пользователя. Правила самозащиты в Интернете : практическое руководство / М. А. Райтман. - Санкт-Петербург : БХВ-Петербург, 2023. - 400 с. - ISBN 978-5-9775-1170-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/2123367.

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) «Введение в информационную безопасность» в рамках текущего контроля успеваемости используются такие виды учебной работы, как лекции, семинары, аудиторная работа, коллоквиум, контрольная работа, 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.

Семинар – это форма учебной деятельности, проводимая в учебном заведении под руководством преподавателя, где студенты активно участвуют в обсуждениях, практических заданиях и других формах взаимодействия.

Для успешной подготовки к семинару рекомендуется заранее ознакомиться с темой занятия и основными материалами, чтобы иметь возможность активно участвовать в обсуждении. Также полезно подготовить вопросы и идеи для обсуждения, что поможет глубже понять материал и продемонстрировать заинтересованность.

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.

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.

Контрольная работа – письменная работа с набором задач, которые нужно решить за ограниченное время.

Цель контрольной работы – получить специальные знания по одной или нескольким темам дисциплины и продемонстрировать навыки их практического применения.

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) «Введение в информационную 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, если иное не указано в силлабусе дисциплины:

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 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
9	Отлично	Зачтено	
8	Отлично	Зачтено	

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
			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) «Введение в информационную безопасность» оценивается следующим образом:

Активность	Вес	Количество	Описание
Контрольная работа	10%	1	Письменная работа с набором задач, которые нужно решить за ограниченное время
Коллоквиум	40%	1	Устные ответы на вопросы, список которых известен студенту заранее
Аудиторная работа	10%	1	Активная работа студента на занятии

Активность	Вес	Количество	Описание
Зачет с оценкой	40%	1	Письменная или устная работа над заданием, направленным на проверку полученных знаний и навыков по дисциплине (модулю)

Формула расчёта итоговой оценки по дисциплине (модулю) «Введение в информационную безопасность»: «0,4 × контрольная работа + 0,4 × коллоквиум + 0,1 × аудиторная работа + 0,4 × зачет с оценкой».

Текущий контроль успеваемости обучающихся по дисциплине (модулю)

Примерные вопросы для подготовки к занятиям

Вопросы к семинару по теме «Понятийный аппарат, методология и контекст»

1. Какие основные понятия входят в базовый аппарат информационной безопасности (конфиденциальность, целостность, доступность)?
2. В чем суть риск-ориентированного подхода к защите информации?
3. Какие этапы включает жизненный цикл атаки (Kill Chain)?
4. Каковы основные процессы реагирования на инциденты информационной безопасности?
5. Какие правовые основы регулируют защиту информации в Российской Федерации?

Вопросы к семинару по теме «Атаки на пользователя и базовая защита»

1. Какие виды социальной инженерии наиболее распространены в корпоративной среде?
2. Каковы признаки фишинговой атаки и методы защиты от нее?
3. Какие типы вредоносного программного обеспечения существуют и каковы их особенности?
4. В чем различие между аутентификацией, авторизацией и идентификацией?
5. Как осуществляется управление секретами и доступами в проекте разработки?

Вопросы к семинару по теме «Инструменты криптографии»

1. В чем разница между симметричным и асимметричным шифрованием?
2. Какие основные алгоритмы симметричного шифрования используются на практике (AES, DES)?
3. Как работает алгоритм RSA и какова его математическая основа?
4. Что такое цифровая подпись и как она обеспечивает целостность данных?
5. Какие существуют методы управления криптографическими ключами?

Примерные вопросы для коллоквиума

Коллоквиум по теме «Основы безопасности и защита от атак»

1. Дайте определение информационной безопасности и назовите ее ключевые свойства.
2. Опишите модель угроз и ее роль в построении системы защиты.
3. Перечислите основные этапы расследования инцидента безопасности.
4. Какие психологические приемы используют злоумышленники в социальной инженерии?
5. Опишите механизм действия программ-вымогателей (ransomware).
6. Какие методы аутентификации обеспечивают наибольший уровень защиты?
7. Каковы принципы управления доступом (DAC, MAC, RBAC)?
8. Приведите пример реальной атаки методом фишинга и ее последствия.
9. Какие организационные меры помогают защититься от вредоносного ПО?

10. Разработайте инструкцию для пользователя при подозрении на заражение компьютера.

Примерные задания для контрольной работы

Вопрос 1. Укажите основной стандарт системы менеджмента информационной безопасности.
Ответ: ISO/IEC 27001

Вопрос 2. Назовите тип атаки социальной инженерии через электронную почту.
Ответ: Фишинг (Phishing)

Вопрос 3. Укажите категорию вредоносного ПО, блокирующего доступ к данным.
Ответ: Ransomware (программы-вымогатели)

Вопрос 4. Назовите метод аутентификации с использованием двух факторов.
Ответ: Двухфакторная аутентификация (2FA)

Вопрос 5. Укажите математическую основу алгоритма RSA.
Ответ: Теория чисел (разложение на множители)

Вопрос 6. Назовите алгоритм симметричного шифрования с блочной структурой.
Ответ: AES (Advanced Encryption Standard)

Вопрос 7. Укажите протокол обмена ключами без предварительного секрета.
Ответ: Диффи-Хеллман (Diffie-Hellman)

Вопрос 8. Назовите систему мониторинга событий безопасности.
Ответ: SIEM (Security Information and Event Management)

Вопрос 9. Укажите технологию предотвращения утечек данных.
Ответ: DLP (Data Loss Prevention)

Вопрос 10. Дайте точное определение вредоносного программного обеспечения.
Ответ: Malware (вредоносное программное обеспечение)

Задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ	Компетенция
1	Укажите модель для оценки рисков безопасности.	Модель угроз (Threat Model)	УК-1
2	Назовите этапы жизненного цикла атаки (Kill Chain).	Разведка / Вторжение / Эксплуатация / Закрепление / Действия	УК-1
3	Укажите правовой акт РФ в области защиты информации.	152-ФЗ «О персональных данных»	УК-1
4	Назовите принцип управления доступом на основе ролей.	RBAC (Role-Based Access Control)	УК-1
5	Укажите вероятностную модель для оценки угроз.	Байесовская сеть (Bayesian Network)	ОПК-1
6	Назовите математическую структуру, используемую в AES.	Конечные поля (Galois Fields)	ОПК-1
7	Укажите концепцию дискретной математики для криптографии.	Модульная арифметика	ОПК-1

Электронный документ

8	Назовите метод количественной оценки рисков.	Quantitative Risk Assessment	ОПК-1
9	Укажите функцию обеспечения целостности данных.	Криптографическая хеш-функция	ОПК-1
10	Назовите инструмент для тестирования на проникновение.	Metasploit Framework	ОПК-6
11	Укажите документ для реагирования на инциденты.	План реагирования (Incident Response Plan)	ОПК-6
12	Назовите метод обнаружения вторжений в сеть.	IDS (Intrusion Detection System)	ОПК-6
13	Укажите тип уязвимости веб-приложений по OWASP.	SQL Injection / XSS	ОПК-6
14	Назовите метод защиты от MITM-атак.	TLS / SSL шифрование	ОПК-6
15	Укажите принцип работы инфраструктуры открытых ключей.	Доверие через цепочку сертификатов (Trust Chain)	ПК-1
16	Назовите стандарт защиты персональных данных в ЕС.	GDPR (General Data Protection Regulation)	ПК-1
17	Укажите инвариант в модели угроз безопасности.	Инвариант безопасности (Security Invariant)	ПК-1
18	Назовите угрозу для систем машинного обучения.	Adversarial Attack (состязательная атака)	ПК-1
19	Укажите метод верификации цифрового контента.	Цифровая подпись / Водяные знаки	ПК-1
20	Назовите этап цифровой криминалистики.	Сбор доказательств / Анализ / Документирование	ПК-1