ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 025053D20009B2A5B043583E315FEF31AD
Владелец: Ивашкевич Евгений Васильевич
Действителен: с 14.10.2024 до 14.01.2026

УТВЕРЖДЕНА

Приказом Ректора АНО ВО
«Центральный университет»
Е.В. Ивашкевич
от «26» июня 2025 г. № 0626.32

Рабочая программа дисциплины (модуля) «Информационная безопасность» дополнительной профессиональной программы – программы профессиональной переподготовки «Академия data science»

Траектория: Backend-разработка

Москва
2025

Электронный документ

Содержание

1. Краткая характеристика дисциплины (модуля)

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.

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

Задачи изучения дисциплины (модуля):

- изучить методы выявления и анализа угроз безопасности в программных продуктах;
- освоить применение криптографических технологий для защиты данных и аутентификации;
- развить умение разрабатывать безопасное программное обеспечение с учетом современных требований;
- научиться оценивать риски и выбирать эффективные стратегии защиты информации;
- приобрести навыки использования специализированных инструментов для тестирования и повышения безопасности приложений.

В результате освоения дисциплины (модуля) обучающийся должен:

знать:

- основные принципы и методы обеспечения информационной безопасности программных систем;
- современные криптографические алгоритмы и их применение в разработке;
- распространённые типы уязвимостей и угроз для веб-приложений и системного уровня.

уметь:

- обнаруживать и анализировать типовые уязвимости в веб-приложениях и системах;
- формулировать и реализовывать базовые меры защиты информации на уровне приложения и системы;
- оценивать риски, связанные с реализацией функциональности, и делать выбор в пользу безопасных решений.

владеть:

- навыками разработки программного обеспечения с учётом требований безопасности;
- навыками применения криптографических механизмов (шифрования, хеширования, цифровой подписи) в программных решениях;
- навыками использования инструментов для оценки безопасности и тестирования приложений.

2. 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)	Консультации			
1	Основные криптографические алгоритмы	2	7			37	Домашние задания Пентесты
2	Безопасность на уровне операционной системы	2	7			37	Домашние задания Пентесты
3	Безопасность веб-приложений	3	7			37	Домашние задания
4	Организационные аспекты информационной безопасности	2	8			37	Домашние задания Пентесты
	Зачет с оценкой				4		
	Итого:	***9***	***29***		***4***	***148***	
Объем дисциплины (модуля) (в ак. ч.)		***190***					

3. Содержание дисциплины (модуля)

№п/п	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам
1	Основные криптографические алгоритмы	Основы криптографии. Генератор псевдослучайных чисел. Метод оценки эффективности ГПСЧ Сеть Фейстеля. Хэши. Коллизии хэшей и радужные таблицы Блочные шифры. AES как пример блочного шифра. Ассиметричное шифрование и цифровая подпись. Алгоритм RSA, Diffie-Helman.
2	Безопасность на уровне операционной системы	Управление доступом в Linux. Пользователи и их права. DAC модель, ACL PAM как средство авторизации в систему. Механизм TOTP. Настройка аудита Изоляция в Linux. CGroups, Namespaces, Capabilities. Бинарные уязвимости и эксплуатация libc Безопасность сетевого стека Linux. Интерфейсы, туннели, firewall, теория PKI и работы сертификатов
3	Безопасность веб-приложений	Теория и практика Web уязвимостей. SQL injection, CSRF, path traversial, XSS Теория и практика Web уязвимостей. RCE, LFI, SSTI, IDOR, SSRF, DoS и Race Conditions
4	Организационные аспекты информационной безопасности	Протокол авторизации и аутентификации. Рассматриваем варианты на основе LDAP и KeyCloak. OIDC и OpenID Spring Security Инфраструктура хранения секретов. Vault Основы контейнерной безопасности. Container Escapes

4. Учебно-методическое обеспечение

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

Каждый слушатель 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.

Слушателям 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.

5. 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
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

6. 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, консультации, домашние задания, пентесты, 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 слушатели 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.

Консультации – структурированные встречи, на которых преподаватели предоставляют индивидуальную или групповую помощь в освоении учебного материала, обсуждении вопросов и решении проблем, возникающих в процессе обучения.

Консультации могут включать разъяснение сложных тем, подготовку к экзаменам и помощь в выполнении проектных работ, что способствует более глубокому пониманию предмета и улучшению академической успеваемости.

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.

Пентесты (penetration testing) – это практика проверки приложений или систем на уязвимости путём имитации действий злоумышленника. Это контролируемая “взлом-сессия”, цель которой не разрушить, а найти слабые места, прежде чем их найдут настоящие

атакующие.

Бонусные баллы — это оценки, которые слушатели могут получить за выполнение дополнительных заданий.

Формат бонусных баллов позволяет слушателям улучшить общую оценку по дисциплине (модулю) и стимулирует углубленное изучение материала.

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

В процессе самостоятельной работы слушатели взаимодействуют с рекомендованными материалами при минимальном участии преподавателя. Задачи слушателя 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)

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***.

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	Слушатель 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. Слушатель 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	Слушатель обладает знаниями предмета почти в полном объеме рабочей
6	Хорошо	Зачтено	

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
			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. Слушатель хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты предмета с практическими задачами.
5	Удовлетворительно	Зачтено	Слушатель 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. Слушатель способен решать только самые простые задачи и владеет лишь минимальным набором методов исследования.
4	Удовлетворительно	Зачтено	
3	Не сдан	Не зачтено	Слушатель 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	40%	За каждое из заданий можно набрать 10 баллов
Пентесты	30%	Практика проверки приложений или систем на уязвимости путём имитации действий злоумышленника
Зачет с оценкой	30%	Письменная или устная работа над заданием, направленным на проверку полученных знаний и навыков по дисциплине (модулю)

В рамках изучения дисциплины (модуля) возможно получение бонусных баллов.

Формула расчёта итоговой оценки по дисциплине (модулю) «Информационная безопасность»: «0,4 × среднее за домашние задания + 0,3 × среднее за пентесты + 0,3 × зачет с оценкой».

Текущий контроль успеваемости обучающихся по дисциплине (модулю)

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 описания заданий для пентестов

1. **Пентест на слабость криптографических реализаций:** Слушатель получает доступ к учебному приложению, использующему AES-шифрование для хранения данных. Задача: имитировать атаку на слабый ключ или уязвимость в генераторе псевдослучайных чисел (например, предсказуемость на основе радужных таблиц), расшифровать данные и предложить улучшения (например, использование более сильных ключей или RSA для

цифровой подписи). Критерии: успешная декодировка, анализ коллизий хэшей, отчет с рекомендациями.

2. **Пентест на управление доступом и изоляцию в Linux:** Слушатель получает виртуальную машину с Linux, где настроены DAC/ACL и CGroups. Задача: имитировать эксплуатацию бинарных уязвимостей (например, через libc) для повышения привилегий, обхода namespaces или capabilities, а также проверить настройки PAM и TOTP. Критерии: обнаружение уязвимостей в аудите, демонстрация успешной эскалации прав, предложения по усилению firewall и PKI-сертификатов.

3. **Пентест на сетевую безопасность Linux:** Слушатель работает с сетевым стеком Linux (интерфейсы, туннели). Задача: имитировать атаку на firewall или сертификаты, используя уязвимости в сетевых интерфейсах (например, подмена сертификатов), и проверить изоляцию через namespaces. Критерии: успешная эксплуатация, анализ логов аудита, рекомендации по настройке туннелей и PKI.

4. **Пентест на инъекции и XSS:** Слушатель получает учебное веб-приложение. Задача: имитировать SQL injection, XSS или CSRF для извлечения данных или выполнения несанкционированных действий, а также проверить на path traversal и RCE. Критерии: успешная эксплуатация уязвимостей, демонстрация LFI/SSTI/IDOR, отчет с мерами защиты (например, фильтрация вводов).

5. **Пентест на DoS и SSRF:** Слушатель тестирует веб-приложение на уязвимости типа DoS, Race Conditions или SSRF. Задача: имитировать атаки для вызова отказов в обслуживании или доступа к внутренним ресурсам, анализируя сетевые взаимодействия. Критерии: воспроизведение атак, оценка рисков, предложения по ограничению запросов.

6. **Пентест на аутентификацию и авторизацию:** Слушатель получает систему с LDAP/KeyCloak или Spring Security. Задача: имитировать обход OIDC/OpenID или эксплуатацию уязвимостей в протоколе авторизации (например, подмена токенов), а также проверить инфраструктуру секретов в Vault. Критерии: успешная несанкционированная аутентификация, анализ рисков, рекомендации по усилению.

7. **Пентест на контейнерную безопасность:** Слушатель работает с контейнерами (Docker/Kubernetes). Задача: имитировать container escape через уязвимости в изоляции или секретах, проверяя управление доступом и хранение данных в Vault. Критерии: демонстрация выхода из контейнера, оценка рисков, предложения по настройке безопасности (например, ограничение capabilities).

Задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ
1.	Какой из перечисленных алгоритмов относится к симметричному шифрованию? а) RSA б) AES в) Диффи-Хеллман г) Эллиптические кривые	б
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
3.	Какой метод наиболее эффективен для защиты веб-приложения от CSRF-атак? а) Использование HTTPS б) Внедрение токенов CSRF	б

	в) Использование сложных паролей г) Ограничение доступа по IP	
4.	Назовите алгоритм асимметричного шифрования, основанный на свойствах эллиптических кривых.	Эллиптические кривые (ECC)
5.	Как называется протокол, позволяющий двум сторонам безопасно обмениваться ключами через незащищённый канал?	Диффи-Хеллман
6.	Какой элемент безопасности ОС отвечает за проверку личности пользователя?	Аутентификация
7.	Как называется процесс управления временем жизни пользователя в веб-приложении после входа в систему?	Управление сессиями
8.	Как называется документ, регламентирующий требования и правила по информационной безопасности в организации?	Политика безопасности
9.	Назовите инструмент для хранения секретов, важный для самооценки инфраструктуры безопасности.	Vault
10.	Назовите сеть, используемую в блочных шифрах.	Фейстель / Feistel
11.	Назовите метод для взлома хэшей с использованием радужных таблиц.	радужные таблицы / rainbow tables
12.	Назовите модель управления доступом в Linux.	DAC / discretionary access control
13.	Назовите механизм авторизации в Linux.	PAM
14.	Назовите технологию изоляции в Linux.	Namespaces / namespaces
15.	Назовите тип уязвимостей, связанных с libc.	бинарные уязвимости / binary vulnerabilities
16.	Назовите тип веб-уязвимости для инъекции SQL.	SQL injection
17.	Назовите тип веб-уязвимости для выполнения кода.	RCE / remote code execution
18.	Назовите тип веб-уязвимости для обхода каталогов.	path traversal
19.	Назовите протокол для аутентификации.	OIDC / OpenID Connect
20.	Назовите фреймворк для безопасности приложений.	Spring Security