Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 23.03.2026 16:20:40
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
«Информационные технологии»
_____ / Д.Г.Демидов /
«15» февраля 2024г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информации в системах обработки данных»

Направление подготовки
10.04.01 «Информационная безопасность»

Профиль
«Системы управления информационной безопасностью»

Квалификация
Магистр

Формы обучения
Очная

Москва, 2024 г.

Разработчик(и):
Доцент кафедры «Информационная безопасность»,
к.т.н, доцент:

 / И.В. Калуцкий /

Согласовано:

Заведующий кафедрой «Информационная безопасность»  И.В.Калуцкий

Руководитель образовательной программы
Доцент. к.т.н.

 /С.А. Кесель/

Содержание

1	Цели, задачи и планируемые результаты обучения по дисциплине	4
2	Место дисциплины в структуре образовательной программы	6
3	Структура и содержание дисциплины	6
3.1	Виды учебной работы и трудоемкость	6
3.2	Тематический план изучения дисциплины	7
3.3	Содержание дисциплины	8
3.4	Тематика семинарских/практических и лабораторных занятий	11
3.5	Тематика курсовых проектов (курсовых работ)	13
4	Учебно-методическое и информационное обеспечение	13
4.1	Нормативные документы и ГОСТы	13
4.2	Основная литература	16
4.3	Дополнительная литература	17
4.4	Электронные образовательные ресурсы	17
4.5	Лицензионное и свободно распространяемое программное обеспечение	17
4.6	Современные профессиональные базы данных и информационные справочные системы	17
5	Материально-техническое обеспечение	17
6	Методические рекомендации	18
6.1	Методические рекомендации для преподавателя по организации обучения	18
6.2	Методические указания для обучающихся по освоению дисциплины	18
7	Фонд оценочных средств	19
7.1	Методы контроля и оценивания результатов обучения	19
7.2	Шкала и критерии оценивания результатов обучения	27
7.3	Оценочные средства	28

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Защита информации в системах обработки данных» следует отнести:

формирование у слушателей необходимого объема теоретических и практических знаний о технологии облачных вычислений, умений и навыков практической реализации облачных технологий для хранения и обработки данных, изучение инструментальных средств данной технологии и методов защиты.

К **основным задачам** освоения дисциплины «Защита информации в системах обработки данных» следует отнести:

1) Рассмотреть методы и способы защиты Государственной тайны, Коммерческой тайны и Персональных данных.
2) Рассмотреть базовые дискреционные, мандатные модели безопасности, модели ролевого управления доступом.
3) Рассмотреть базовую модель изолированной программной среды.
4) Рассмотреть базовые модели безопасности информационных потоков в облачной инфраструктуре и методы защиты данных.

Обучение по дисциплине **«Защита информации в системах обработки данных»** направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-1. Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	ИПК-1.1. Применяет знания направлений развития информационных технологий, основных видов политик безопасности объектов защиты; ИПК-1.2. Умеет прогнозировать эффективность функционирования, оценивать затраты и риски объектов защиты; ИПК-1.3. Владеет навыками формирования политики безопасности объектов защиты
ПК-4. Способен разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	ИПК-4.1. Знает: программы и методики испытаний средств и систем обеспечения информационной безопасности в соответствии с нормативными актами. ИПК-4.2. Умеет: разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности ИПК-4.3. Владеет: навыками проведения испытаний средств и систем обеспечения информационной безопасности

2 Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации в системах обработки данных» относится к числу профессиональных учебных дисциплин обязательной части базового цикла (Б1.1) основной образовательной программы магистратуры (Б1.1.2)

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Управление информационной безопасностью», «Построение и совершенствование систем управления информационной безопасностью»,

«Производственная практика (научно-исследовательская работа)», «Производственная практика (проектно-технологическая)», «Производственная практика (преддипломная)».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных(е) единиц(ы) (180 часов) во втором семестре.

1. Виды учебной работы и трудоемкость
(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**80**	1	1-18
	В том числе:			
1.1	Лекции	16		
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	64	1	1-18
2	**Самостоятельная работа**	**100**	1	1-18
3	**Промежуточная аттестация**	**Экзамен, курсовой проект**	Экзамен, курсовой проект	По расписанию
	Итого:	**180**		

2. Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Тема 1. Безопасность персональных данных в автоматизированных системах	10	2				8
2	Тема 2. Защита данных, составляющих государственную тайну	10	2				8
3	Тема 3. Защита данных, составляющих коммерческую тайну	14	2				12
4	Тема 4. Защита данных в облачной инфраструктуре	48	4		20		24
5	Тема 5. Серверы в облаке и центры обработки данных	50	2		24		24
6	Тема 6. Управление доступом в инфраструктуре Yandex Cloud	48	4		20		24
Итого		180	16		64		100

3. Содержание дисциплины

Тема 1. Безопасность персональных данных в автоматизированных системах.
Тема 2. Защита данных, составляющих государственную тайну.
Тема 3. Защита данных, составляющих коммерческую тайну.
Тема 4. Защита данных в облачной инфраструктуре.
Тема 5. Серверы в облаке и центры обработки данных.
Тема 6. Управление доступом в инфраструктуре Yandex Cloud.

4. Тематика семинарских/практических и лабораторных занятий

Семинарские/практические занятия в учебном плане не запланированы.

4.1 Лабораторные занятия

1. Лабораторная работа № 1 «Подготовка тестовой инфраструктуры»
2. Лабораторная работа № 2«Группы безопасности»
3. Лабораторная работа № 3 «Защищённое соединение с облаком»
4. Лабораторная работа № 4 «Доступ пользователей»
5. Лабораторная работа № 5 «Сбор и анализ событий безопасности»
6. Лабораторная работа № 6 «Отказоустойчивые кластеры баз данных»

5. Тематика курсовых проектов (курсовых работ)

Курсовые проект выполняется в 1 семестре и является обязательным условием допуска к экзамену.

6. Учебно-методическое и информационное обеспечение

6.1 Нормативные документы и ГОСТы

1. "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)
2. ГОСТ Р 53131-2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения».
3. ГОСТ Р ИСО/МЭК 27005-2010 Национальный стандарт российской федерации информационная технология методы и средства обеспечения безопасности менеджмент риска информационной безопасности
4. "ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

5. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности»

6.2 Основная литература

1) Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва : РУТ (МИИТ), 2019. — 144 с. — ISBN 978-5-7876-0326-2. — Текст :
2) электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/188703
3) Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания : учебное пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. — Ростов-на-Дону : ИУБиП, 2020. — 114 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/248747
4) Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401
5) Потерпеев, Г. Ю. Безопасность операционных систем : учебное пособие / Г. Ю. Потерпеев, В. С. Нефедов, А. А. Криулин. — Москва : РТУ МИРЭА, 2021. — 93 с. — ISBN 978-5-7339-1393-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182416

6.3 Дополнительная литература

1) Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. —URL: https://urait.ru/bcode/512269
2) «Защита информационных процессов в компьютерных системах» (Пушкарёв, В. В. Защита информационных процессов в компьютерных системах : учебное пособие / В. В. Пушкарёв, В. П. Пушкарёв. — Москва : ТУСУР, 2012. — 131 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4925
3) Особенности обеспечения безопасности персональных данных в автоматизированных системах. [Электронный ресурс]. — Режим доступа: https://studfile.net/preview/6802020/page:2/
4) Защита государственной тайны в РФ: практическое руководство [Электронный ресурс]. — Режим доступа: https://cisoclub.ru/zashhita-gosudarstvennoj-tajny-v-rf-prakticheskoe-rukovodstvo/
5) Защита информации, составляющей коммерческую тайну [Электронный ресурс]. — Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/zaschita-informatsii-sostavlyayuschej-kommercheskuyu-tajnu/
6) Что такое безопасность облака? [Электронный ресурс]. — Режим доступа: https://www.trendmicro.com/ru_ru/what-is/cloud-security.html
7) Аллен, П. Дж. (Пол Дж.) Руководство по архитектуре облачных приложений / Пол Дж. Аллен ; [пер. с англ. А. Ю. Шелестова]. — Москва : ДМК Пресс, 2020. — 430 с.

8) Функции архитектуры безопасности облака [Электронный ресурс]. — Режим доступа: https://learn.microsoft.com/ru-ru/azure/cloud-adoption-framework/organize/cloud-security-architecture, свободный. — Загл. с экрана. — Яз. рус. (Дата обращения: 10.08.2023).
9) Документация Yandex Cloud [Электронный ресурс]. — Режим доступа: https://cloud.yandex.ru/docs — Загл. с экрана. — Яз. рус. (Дата обращения: 10.08.2023).
10) Инженер облачных сервисов. Образовательный курс [Электронный ресурс]. — Режим доступа: https://practicum.yandex.ru/ycloud/ — Загл. с экрана. — Яз. рус. (Дата обращения: 10.08.2023).
11) Защита облачной инфраструктуры. Образовательный курс [Электронный ресурс]. — Режим доступа: https://yandex.cloud/ru/training/infrastructure-protection — Загл. с экрана. — Яз. рус. (Дата обращения: 10.08.2023).

6.4 Электронные образовательные ресурсы

1. ЭОР – «Защита информации в системах обработки данных» [Электронный ресурс]. — Режим доступа: https://online.mospolytech.ru/course/view.php?id=14300.
2. Московский Политех подключен к ЭБС: Юрайт, АйПиАр и Лань
3. Электронно-библиотечные системы [Электронный ресурс]. — Режим доступа: https://mospolytech.ru/obuchauschimsya/biblioteka/

6.5 Лицензионное и свободно распространяемое программное обеспечение

Для выполнения лабораторных работ и самостоятельной работы необходимо следующее программное обеспечение:

1. Microsoft Windows.
2. Веб-браузер, Chrome.

6.6 Современные профессиональные базы данных и информационные справочные системы

1. Справочная правовая система "КонсультантПлюс" https://www.consultant.ru/
2. Официальный сайт ФСТЭК России https://fstec.ru/
3. Образовательная платформа «Юрайт» https://urait.ru/

7. Материально-техническое обеспечение

И лекционные и лабораторные занятия могут проводится дистанционно в формате онлайн. Преподавателю для проведения занятий необходим ноутбук с возможностью использования сервиса корпоративной платформы Microsoft Teams или других платформ для проведения занятий, например, Webinar. У студентов должна быть возможность выхода в Интернет.

8. Методические рекомендации

1. Методические рекомендации для преподавателя по организации обучения

При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

2. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов помогает получить дополнительные теоретические и практические знаниями по изучаемой дисциплине, развивает сознательное отношение к интеллектуальному труду.

В процессе самостоятельной работы, студенты дорабатывают конспекты лекций, готовятся к экзамену, изучают рекомендованную литературу, осуществляют подборку нормативно-правовых документов и проводят ознакомительный анализ с ними, готовятся к лабораторным работам, выполняют домашние задания;

Самостоятельная работа позволяет закрепить и углубить знания, полученные во время аудиторных занятий, а также изучить отдельные темы учебной программы.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Лекционные занятия дают общее представление по изучаемой теме, основной знания студент получает в процессе выполнения лабораторных работ и самостоятельной работы.

Практические занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ.

Домашним заданием, по большей части, является подготовка к следующей лабораторной работе. Студентам предлагается выполнить подбор литературы, нормативно-правовых документов, по тематике лабораторной работы, и предварительное ознакомление с ними.

При проведении лабораторной работы преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, отвечает на вопросы студентов, проверяет выполненные работы. На следующем занятии, подводится итог проведенной работы, студентам сообщаются результаты, ведется обсуждение рассмотренных вопросов подводится итог занятию в целом.

По результатам выполнения всех видов учебной работы, предусмотренных учебным планом (подготовка конспектов лекций, успешное выполнение лабораторных работ, подготовка домашнего задания, присутствие и активная работа на занятиях) по данной дисциплине (модулю), преподаватель может рассмотреть возможность проставления положительной оценки на экзамене «Автоматом», при этом учитываются результаты текущего контроля успеваемости в течение семестра. В случае, если студент длительно отсутствовал на занятиях, не выполнял задания он всё равно допускается до экзамена, но на экзамене, таким студентам, преподаватель может задавать любое количество вопросов по всем темам данной дисциплины (в рамках отведённого времени), дабы убедиться, что студент самостоятельно освоил дисциплину.

Текущий контроль осуществляется на практических занятиях, промежуточный

контроль осуществляется на экзамене в письменной (устной) форме.

9. Фонд оценочных средств

1. Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- домашние задания и их защита;
- лабораторные работы
- дифференцированный зачёт.

2. Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю)

ПК-1. Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: направления развития информационных (телекоммуникационных) технологий	Обучающийся демонстрирует полное отсутствие знаний направлений развития информационных (телекоммуникационных) технологий	Обучающийся демонстрирует неполное знание направлений развития информационных (телекоммуникационных) технологий	Обучающийся демонстрирует частичное знание направлений развития информационных (телекоммуникационных) технологий	Обучающийся демонстрирует полное знание направлений развития информационных (телекоммуникационных) технологий
уметь: прогнозировать эффективность функционирования объектов защиты	Обучающийся не умеет прогнозировать эффективность функционирования объектов защиты	Обучающийся демонстрирует неполное умение прогнозировать эффективность функционирования объектов защиты	Обучающийся демонстрирует частичное умение прогнозировать эффективность функционирования объектов защиты	Обучающийся демонстрирует полное умение прогнозировать эффективность функционирования

				объектов защиты
владеть: методами оценки затрат и рисков, формирования политик безопасности объектов защиты	Обучающийся не владеет методами оценки затрат и рисков, формирования политик безопасности объектов защиты	Обучающийся в неполном объеме владеет методами оценки затрат и рисков, формирования политик безопасности объектов защиты	Обучающийся частично владеет методами оценки затрат и рисков, формирования политик безопасности объектов защиты	Обучающийся в полном объеме владеет методами оценки затрат и рисков, формирования политик безопасности объектов защиты
ПК-4. Способен разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности				
знать: принципы разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует полное отсутствие знаний принципов разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует неполное знание принципов разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует частичное знание принципов разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует полное знание принципов разработки программ и методик испытаний средств и систем обеспечения информационной безопасности

уметь: использовать программы и методики испытаний средств и систем обеспечения информационной безопасности	Обучающийся не умеет использовать программы и методики испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует неполное умение использовать программы и методики испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует частичное умение использовать программы и методики испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует полное умение использовать программы и методики испытаний средств и систем обеспечения информационной безопасности
владеть: принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся не владеет принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся в неполном объеме владеет принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся частично владеет принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся в полном объеме владеет принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен

Промежуточная аттестация обучающихся, в форме экзамена, проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

3. Оценочные средства

7.3.1. Примерный список вопросов для экзамена

1. Особенности обеспечения безопасности персональных данных в автоматизированных системах
2. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных
3. Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн
4. Основные принципы обеспечения безопасности персональных данных
5. Практическая защита гостайны
6. Аттестация на соответствие требованиям по защите государственной тайны
7. Аттестационные испытания
8. Угрозы коммерческой тайне
9. Способы получения информации, составляющей коммерческую тайну
10. Меры защиты коммерческой тайны
11. Обеспечение безопасности облачной среды
12. Подходы к обеспечению безопасности облака
13. Риски для безопасности облака
14. Облачное хранилище и общий доступ к файлам
15. Облачный сервер
16. Как выбрать провайдера облачных услуг
17. S3 - Simple Storage Service
18. Соглашение об уровне обслуживания (SLA)
19. Введение в систему классификации TIER
20. Назначение сервиса Terraform
21. Защита подключения к облачной инфраструктуре
22. Группы безопасности в Yandex Cloud
23. Использование VPN в облачной инфраструктуре

24. Управление доступом пользователей в облачной инфраструктуре Yandex Cloud
25. Понятие «Федерации» в Yandex Cloud, примеры использования
26. Логирование событий в Yandex Cloud, примеры
27. Система контроля событий безопасности в Yandex Cloud, примеры
28. Отказоустойчивые кластеры, виды, назначение.

7.3.2 Примерный список тем для курсового проектирования

Криптографические методы защиты

1. Разработка протокола распределения ключей для групповой работы в системах обработки данных.
2. Исследование методов постквантовой криптографии в системах обработки больших данных
3. Реализация гибридной криптосистемы для защиты транзакций в блокчейн-сетях
4. Анализ угроз целостности данных в системах распределенного реестра (Blockchain)
5. Реализация и оценка механизмов слепой подписи для систем анонимного голосования

Системы обнаружения вторжений

6. Создание системы обнаружения аномалий в потоках Big Data
7. Исследование методов детектирования APT-атак в корпоративных системах
8. Реализация системы поведенческого анализа для защиты баз данных
9. Разработка SIEM-решения для мониторинга безопасности хранилищ данных
10. Моделирование атак типа "злоумышленник-посредник" (Man-in-the-Middle) в протоколах взаимодействия IoT-устройств

Защита баз данных

11. Внедрение методов шифрования на уровне столбцов в корпоративных СУБД
12. Разработка системы контроля доступа к данным на основе атрибутивной модели
13. Исследование методов маскирования данных в распределенных системах
14. Создание системы аудита действий пользователей в многопользовательских БД
15. Реализация политики наименьших привилегий в системах управления данными

Безопасность облачных решений

16. Методы и средства контроля доступа на основе атрибутов (ABAC) в гибридных облачных инфраструктурах
17. Исследование методов безопасной миграции данных между облачными провайдерами
18. Разработка модели управления ключами шифрования для мультитенантных SaaS-решений
19. Реализация политики нулевого доверия в облачных инфраструктурах
20. Разработка системы резервного копирования с гарантированной защитой данных

Защита больших данных

21. Исследование методов безопасной агрегации данных в Hadoop
22. Разработка системы защиты потоковых данных в Apache Kafka
23. Создание решения для безопасной обработки конфиденциальных данных в Spark
24. Реализация политики конфиденциальности в системах машинного обучения
25. Исследование методов защиты метаданных в системах управления данными

Безопасность приложений

26. Разработка системы защиты API для доступа к данным

27. Создание фреймворка безопасной обработки данных в микросервисах
28. Исследование методов защиты от SQL-инъекций в современных приложениях
29. Реализация системы защиты от DDoS-атак на базы данных
30. Разработка решения для безопасной обработки персональных данных

Управление рисками

31. Создание системы оценки рисков утечки данных в корпоративных системах
32. Исследование методов количественной оценки рисков в облачных сервисах
33. Разработка методики оценки уязвимостей в системах хранения данных
34. Реализация системы прогнозирования инцидентов безопасности
35. Создание модели управления рисками в распределенных системах обработки данных

Защита данных на протяжении всего жизненного цикла

36. Система мониторинга целостности данных в распределенных системах хранения.
37. Методы безопасного удаления (sanitization) данных с современных устройств хранения (SSD, NVMe).
38. Разработка политики управления жизненным циклом ключей шифрования (Key Lifecycle Management) для крупной организации.
39. Обеспечение конфиденциальности и доступности данных в системах аварийного восстановления (Disaster Recovery).
40. Применение технологий Data Loss Prevention (DLP) для контроля потоков данных в корпоративной сети.