Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра автоматики

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Криптография и защита информации

Образовательная программа: 27.04.04 Управление в технических системах, магистерская программа: Комплексные системы автоматизации

Курс: 1, семестр : 2

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**2**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	35
4	Лекции, час.	14
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	14
7	из них в активной и интерактивной форме, час.	28
8	из них практической подготовки, час.	12
9	Аттестация, час.	2
10	Консультации, час.	5
11	Самостоятельная работа, час.	73
12	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ(Р)/реферат, подготовка к контрольной работе)	
13	Вид аттестации	3

Новосибирск 2021

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 27.04.04 Управление в технических системах

ФГОС введен в действие приказом №942 от 11.08.2020 г. , дата утверждения: 21.08.2020 г.

Место дисциплины в структуре учебного плана: Блок 1, формируемая участниками образовательных отношений

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 27.04.04 Управление в технических системах

Рабочая программа обсуждена на заседании кафедры

АВТ, протокол заседания кафедры №_____ от 31.08.2021

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 8 от 31.08.2021

Рабочую программу дисциплины разработал:

доцент, к.ф-м.н. Пестунов А. И.

Заведующий кафедрой:

доцент, д.т.н. Жмудь В. А.

Ответственный за образовательную программу:

заведующий кафедрой Жмудь В. А.

1. Внешние требования

Таблица 1.1

Группа	Компетенции
	Индикаторы достижения компетенций
Профессиональные компетенции	ПК-3.В/НА Способен применять современные методы разработки информационного и алгоритмического обеспечения систем автоматизации и управления
	ПК-3.В/НА. 2 Умеет применять современные технологии обработки информации, компьютерных сетей и телекоммуникаций
Универсальные компетенции	УК-2 Способен управлять проектом на всех этапах его жизненного цикла
	УК-2. 1 Знает особенности управления проектом в зависимости от этапа жизненного цикла

2. Требования НГТУ к планируемым результатам обучения, соотнесенным с индикаторами достижения компетенций

Таблица 2.1

Индикаторы достижения компетенций	Формы организации занятий
Результаты обучения	
ПК-3.В/НА. 2 Умеет применять современные технологии обработки информации, компьютерных сетей и телекоммуникаций	
применять современные технологии обработки информации, компьютерных сетей и телекоммуникаций	Лабораторные работы; Самостоятельная работа
УК-2. 1 Знает особенности управления проектом в зависимости от этапа жизненного цикла	
особенности управления проектом в зависимости от этапа жизненного цикла	Лекции; Лабораторные работы; Самостоятельная работа

3. Содержание и структура дисциплины

Таблица 3.1

Темы лекций	Часы	Из них в форме практ. подг., час.	Активные формы, час.	Индикаторы достижения компетенций	Учебная деятельность
Семестр: 2					
Дидактическая единица: Защита информации и ее место в современном мире.					

1. Понятие информационной безопасности. Конфиденциальность, целостность, доступность. Связь защиты информации и информационной безопасности. Законные и незаконные пользователи. Идентификация, аутентификация и авторизация. Угроза информационной безопасности. Источники угроз. Уязвимость. Атака. Эксплуатация уязвимости. Законодательство в сфере информационной безопасности. Способы защиты информации. Защита информации как комплексная деятельность по обеспечению информационной безопасности.	1	0	1	УК-2.1	Ознакомление с понятием информационной безопасности. Конфиденциальность, целостность, доступность. Связь защиты информации и информационной безопасности. Законные и незаконные пользователи. Идентификация, аутентификация и авторизация. Угроза информационной безопасности. Источники угроз. Уязвимость. Атака. Эксплуатация уязвимости. Законодательство в сфере информационной безопасности. Способы защиты информации. Защита информации как комплексная деятельность по обеспечению информационной безопасности.
Дидактическая единица: Введение в криптографию.					

2. Историческая и современная криптография. Место криптографии в информационной безопасности. Государственные стандарты на криптографические алгоритмы. Криптографические библиотеки в языках программирования. Схема секретной связи Шеннона. Действующие лица в криптографии. Понятие криптографического ключа. Шифр перестановки. Шифр Подстановки. Зашифрование, расшифрование и криптоанализ (на примере шифра Цезаря). Количество возможных ключей и полный перебор. Длина ключа. Шифр Вернама. Сравнение длин ключей различных шифров. Влияние длины ключа на стойкость шифра. Эмпирический закон Мура и длина ключа. Принцип Керкгоффса и его значимость. Сценарии атак на шифрсистемы. Атака на основе шифртекста. Атака на основе известного открытого текста. Атака на основе выбранного открытого/шифрованного текста. Атака на основе адаптивно выбранного открытого/шифрованного текста. Атака на связанные ключи. Программные реализации исторических шифров.	2	0	2	УК-2.1	Ознакомление с исторической и современной криптографией. Место криптографии в информационной безопасности. Государственные стандарты на криптографические алгоритмы. Криптографические библиотеки в языках программирования. Схема секретной связи Шеннона. Действующие лица в криптографии. Понятие криптографического ключа. Шифр перестановки. Шифр Подстановки. Зашифрование, расшифрование и криптоанализ (на примере шифра Цезаря). Количество возможных ключей и полный перебор. Длина ключа. Шифр Вернама. Сравнение длин ключей различных шифров. Влияние длины ключа на стойкость шифра. Эмпирический закон Мура и длина ключа. Принцип Керкгоффса и его значимость. Сценарии атак на шифрсистемы. Атака на основе шифртекста. Атака на основе известного открытого текста. Атака на основе выбранного открытого/шифрованного текста. Атака на основе адаптивно выбранного открытого/шифрованного текста. Атака на связанные ключи. Программные реализации исторических шифров.
Дидактическая единица: Симметричные шифры.					

3. Современные поточные шифры и их связь с шифром Вернама. Шифры RC4 и A5. Линейные регистры сдвига. Краткий обзор конкурса поточных шифров eStream. Программные реализации поточных шифров.	1	0	1	УК-2.1	Ознакомление с современными поточными шифрами и их связь с шифром Вернама. Шифры RC4 и A5. Линейные регистры сдвига. Краткий обзор конкурса поточных шифров eStream. Программные реализации поточных шифров.
4. Блочные шифры. Принципы построения блочных шифров и требования, предъявляемые к ним. Режимы шифрования: ECB, CBC, CFB, OFB, CTR. Свойства режимов шифрования. Блочные шифры DES, ГОСТ 28147-89 "Магма", ГОСТ Р 34.12-2015 "Кузнечик", AES, RC6. Основы криптоанализа блочных шифров. Основные атаки на блочные шифры. Программные реализации блочных шифров. Режимы блочного шифрования OFB, CTR и поточные шифры.	1	0	1	УК-2.1	Ознакомление с блочными шифрами. Принципы построения блочных шифров и требования, предъявляемые к ним. Режимы шифрования: ECB, CBC, CFB, OFB, CTR. Свойства режимов шифрования. Блочные шифры DES, ГОСТ 28147-89 "Магма", ГОСТ Р 34.12-2015 "Кузнечик", AES, RC6. Основы криптоанализа блочных шифров. Основные атаки на блочные шифры. Программные реализации блочных шифров. Режимы блочного шифрования OFB, CTR и поточные шифры.

5. Применение случайных и псевдослучайных чисел в криптографии. Энтропия источника. Методы получения случайных и псевдослучайных последовательностей. Линейный конгруэнтный генератор. Мультипликативный линейный конгруэнтный генератор. Генератор Фибоначчи. Генератор BBS. Комбинированные генераторы. Методы "очищения" псевдослучайных последовательностей Фон Неймана и Элайеса. Использование шифров с секретным ключом для получения псевдослучайных последовательностей. Статистические тесты и их роль. Обзор классических статистических тестов и критериев. Обзор тестов, рекомендованных NIST.	1	0	1	УК-2.1	Ознакомление с применением случайных и псевдослучайных чисел в криптографии. Энтропия источника. Методы получения случайных и псевдослучайных последовательностей. Линейный конгруэнтный генератор. Мультипликативный линейный конгруэнтный генератор. Генератор Фибоначчи. Генератор BBS. Комбинированные генераторы. Методы "очищения" псевдослучайных последовательностей Фон Неймана и Элайеса. Использование шифров с секретным ключом для получения псевдослучайных последовательностей. Статистические тесты и их роль. Обзор классических статистических тестов и критериев. Обзор тестов, рекомендованных NIST.
Дидактическая единица: Теоретические основы асимметричной криптографии.					

6. Примеры задач, не разрешимых в рамках схемы Шеннона. Проблема хранения паролей. Система противовоздушной обороны (система "свой-чужой"). Проблема авторизации и регистрации в системах с удаленным доступом. Подсчет числа симметричных ключей для группы пользователей. Односторонние функции. Быстрый алгоритм возведения в степень по модулю и его сложность. Понятие дискретного логарифма и задача дискретного логарифмирования. Дискретное логарифмирование методом полного перебора. Метод "Шаг младенца, шаг великана". Обоснование того, что при больших числах возведение в степень по модулю является односторонней функцией. "Подсоленные пароли".	1	0	1	УК-2.1	Ознакомление с примерами задач, не разрешимых в рамках схемы Шеннона. Проблема хранения паролей. Система противовоздушной обороны (система "свой-чужой"). Проблема авторизации и регистрации в системах с удаленным доступом. Подсчет числа симметричных ключей для группы пользователей. Односторонние функции. Быстрый алгоритм возведения в степень по модулю и его сложность. Понятие дискретного логарифма и задача дискретного логарифмирования. Дискретное логарифмирование методом полного перебора. Метод "Шаг младенца, шаг великана". Обоснование того, что при больших числах возведение в степень по модулю является односторонней функцией. "Подсоленные пароли".

7. Применение элементов теории чисел в криптографии. Простые числа. Проверка числа на простоту. Решето Эратосфена. Критерий Вильсона. Взаимно простые числа. Основная теорема арифметики. Разложение числа на простые множители. Функция Эйлера. Теоремы Эйлера и Ферма. Вероятностные тесты на простоту. Тест Ферма. Наибольший общий делитель. Наименьшее общее кратное. Алгоритм Евклида. Диофантово уравнение. Обобщенный (расширенный) алгоритм Евклида. Понятие мультипликативной инверсии. Вычисление инверсий с помощью обобщенного алгоритма Евклида. Метод полного перебора. Программные реализации теоретико-числовых алгоритмов.	1	0	1	УК-2.1	Ознакомление с применением элементов теории чисел в криптографии. Простые числа. Проверка числа на простоту. Решето Эратосфена. Критерий Вильсона. Взаимно простые числа. Основная теорема арифметики. Разложение числа на простые множители. Функция Эйлера. Теоремы Эйлера и Ферма. Вероятностные тесты на простоту. Тест Ферма. Наибольший общий делитель. Наименьшее общее кратное. Алгоритм Евклида. Диофантово уравнение. Обобщенный (расширенный) алгоритм Евклида. Понятие мультипликативной инверсии. Вычисление инверсий с помощью обобщенного алгоритма Евклида. Метод полного перебора. Программные реализации теоретико-числовых алгоритмов.
Дидактическая единица: Асимметричные криптосистемы.					
8. Система распределения ключей Диффи-Хеллмана. Шифрсистема Шамира. Шифрсистема Эль-Гамаля. Шифрсистема Мак-Элиса. Односторонняя функция с лазейкой и шифрсистема RSA. Выбор параметров для шифрсистем с открытыми ключами.	1	0	1	УК-2.1	Ознакомление с системами распределения ключей Диффи-Хеллмана. Шифрсистема Шамира. Шифрсистема Эль-Гамаля. Шифрсистема Мак-Элиса. Односторонняя функция с лазейкой и шифрсистема RSA. Выбор параметров для шифрсистем с открытыми ключами.
9. Основные идеи, лежащие в основе электронной цифровой подписи (ЭЦП). Требования к ЭЦП. ЭЦП на основе шифрсистем с открытыми ключами. ЭЦП Эль-Гамаля и RSA. Выбор параметров для ЭЦП. Одноразовые цифровые подписи. Стандарты на ЭЦП: ГОСТ Р34.10-94, ГОСТ Р34.10-2001, FIPS 186, FIPS 186-2.	1	0	1	УК-2.1	Ознакомление с основными идеями, лежащими в основе электронной цифровой подписи (ЭЦП). Требования к ЭЦП. ЭЦП на основе шифрсистем с открытыми ключами. ЭЦП Эль-Гамаля и RSA. Выбор параметров для ЭЦП. Одноразовые цифровые подписи. Стандарты на ЭЦП: ГОСТ Р34.10-94, ГОСТ Р34.10-2001, FIPS 186, FIPS 186-2.

10. Криптографические протоколы. Протоколы идентификации. Атака на систему "Диффи-Хеллмана". Протокол Нидхама-Шредера. Протокол привязки к биту. Игровые протоколы. Протокол подбрасывания монеты по телефону и его иллюстрация. Ментальный покер. Доказательство с нулевым разглашением. Протокол электронного голосования.	1	0	1	УК-2.1	Ознакомление с криптографическими протоколами. Протоколы идентификации. Атака на систему "Диффи-Хеллмана". Протокол Нидхама-Шредера. Протокол привязки к биту. Игровые протоколы. Протокол подбрасывания монеты по телефону и его иллюстрация. Ментальный покер. Доказательство с нулевым разглашением. Протокол электронного голосования.
Дидактическая единица: Криптосистемы на эллиптических кривых.					
11. Асимметричные криптосистемы на эллиптических кривых. Использование М-кратной композиции вместо модульного возведения в степень. Сложение точек. Умножение точки на число. Преимущества криптосистем на эллиптических кривых. Сравнение длин ключей для традиционных асимметричных криптосистем и их аналогов на эллиптических кривых. Криптографические стандарты на эллиптических кривых.	1	0	1	УК-2.1	Ознакомление с асимметричными криптосистемами на эллиптических кривых. Использование М-кратной композиции вместо модульного возведения в степень. Сложение точек. Умножение точки на число. Преимущества криптосистем на эллиптических кривых. Сравнение длин ключей для традиционных асимметричных криптосистем и их аналогов на эллиптических кривых. Криптографические стандарты на эллиптических кривых.
Дидактическая единица: Криптографические хеш-функции.					

12. Определение хеш-функции. Целостность данных и аутентификация сообщений. Криптографические хеш-функции и требования, предъявляемые к ним. Понятие коллизий первого и второго рода. Парадокс дней рождений. Бесключевые хеш-функции и хеш-функции, задаваемые ключом. Построение хеш-функций, задаваемых ключом, на основе бесключевых. Алгоритмы HMAC, UMAC, CBC-MAC. Применение хеш-функций в криптографии. Коды аутентичности сообщений. Хеш-функция MD5 и семейство SHA. Хеш-функции, базирующиеся на блочных шифрах. Краткий обзор конкурса хеш-функций SHA-3. Российские стандарты на криптографическую хеш-функцию ГОСТ Р34.11-94 и ГОСТ Р 34.11-2012. Зарубежные стандарты на криптографические хеш-функции. Возможные атаки на функции хеширования.	1	0	1	УК-2.1	Ознакомление с определением хеш-функции. Целостность данных и аутентификация сообщений. Криптографические хеш-функции и требования, предъявляемые к ним. Понятие коллизий первого и второго рода. Парадокс дней рождений. Бесключевые хеш-функции и хеш-функции, задаваемые ключом. Построение хеш-функций, задаваемых ключом, на основе бесключевых. Алгоритмы HMAC, UMAC, CBC-MAC. Применение хеш-функций в криптографии. Коды аутентичности сообщений. Хеш-функция MD5 и семейство SHA. Хеш-функции, базирующиеся на блочных шифрах. Краткий обзор конкурса хеш-функций SHA-3. Российские стандарты на криптографическую хеш-функцию ГОСТ Р34.11-94 и ГОСТ Р 34.11-2012. Зарубежные стандарты на криптографические хеш-функции. Возможные атаки на функции хеширования.
Дидактическая единица: Элементы стеганографии.					

13. Задача стеганографии. Классическая стеганография. Компьютерная стеганография. Цифровая стеганография. LSB-замещение. LSB-внедрение. Адаптивное внедрение. Задача стегоанализа. Понятие ошибки обнаружение. Размер внедрения. Оценка эффективности методов стегоанализа. Цифровые водяные знаки. Визы цифровых водяных знаков.	1	0	1	УК-2.1	Ознакомление с задачами стеганографии. Классическая стеганография. Компьютерная стеганография. Цифровая стеганография. LSB-замещение. LSB-внедрение. Адаптивное внедрение. Задача стегоанализа. Понятие ошибки обнаружение. Размер внедрения. Оценка эффективности методов стегоанализа. Цифровые водяные знаки. Визы цифровых водяных знаков.

Темы лабораторных работ	Часы	Из них в форме практ. подг., час.	Активные формы, час.	Индикаторы достижения компетенций	Учебная деятельность
Семестр: 2					
Дидактическая единица: Защита информации и ее место в современном мире.					
1. Программная реализация метода полного перебора.	1	1	1	ПК-3.В/НА.2,УК-2.1	Изучение программы реализации метода полного перебора.
Дидактическая единица: Введение в криптографию.					
2. Программная реализация исторических шифров.	2	2	2	ПК-3.В/НА.2,УК-2.1	Изучение программной реализации исторических шифров.
Дидактическая единица: Симметричные шифры.					
3. Программная реализация симметричных шифров.	3	2	3	ПК-3.В/НА.2,УК-2.1	Изучение программной реализации симметричных шифров.
Дидактическая единица: Теоретические основы асимметричной криптографии.					
4. Программная реализация теоретико-числовых алгоритмов.	2	2	2	ПК-3.В/НА.2,УК-2.1	Изучение программной реализации теоретико-числовых алгоритмов.
Дидактическая единица: Асимметричные криптосистемы.					
5. Программная реализация асимметричных криптосистем.	3	2	3	ПК-3.В/НА.2,УК-2.1	Изучение программной реализации асимметричных криптосистем.
Дидактическая единица: Криптосистемы на эллиптических кривых.					
6. Программная реализация М-кратной композиции и криптосистем на эллиптических кривых.	1	1	1	ПК-3.В/НА.2,УК-2.1	Изучение программной реализации М-кратной композиции и криптосистем на эллиптических кривых.
Дидактическая единица: Криптографические хеш-функции.					

7. Программная реализация криптографических хеш-функций.	1	1	1	ПК-3.В/НА.2,УК-2.1	Изучение программной реализации криптографических хеш-функций.
Дидактическая единица: Элементы стеганографии.					
8. Программная реализация методов цифровой стеганографии.	1	1	1	ПК-3.В/НА.2,УК-2.1	Изучение программной реализации методов цифровой стеганографии.

3.1 Практическая подготовка

Таблица 3.2

№	Темы занятий	Формы организации занятий	Содержание практической подготовки (виды работ)
1	Программная реализация метода полного перебора.	Лб	Выполняет следующие виды работ: изучение программы реализации метода полного перебора.
2	Программная реализация исторических шифров.	Лб	Выполняет следующие виды работ: изучение программной реализации исторических шифров.
3	Программная реализация симметричных шифров.	Лб	Выполняет следующие виды работ: изучение программной реализации симметричных шифров.
4	Программная реализация теоретико-числовых алгоритмов.	Лб	Выполняет следующие виды работ: изучение программной реализации теоретико-числовых алгоритмов.
5	Программная реализация асимметричных криптосистем.	Лб	Выполняет следующие виды работ: изучение программной реализации асимметричных криптосистем.
6	Программная реализация М-кратной композиции и криптосистем на эллиптических кривых.	Лб	Выполняет следующие виды работ: изучение программной реализации М-кратной композиции и криптосистем на эллиптических кривых.
7	Программная реализация криптографических хеш-функций.	Лб	Выполняет следующие виды работ: изучение программной реализации криптографических хеш-функций.
8	Программная реализация методов цифровой стеганографии.	Лб	Выполняет следующие виды работ: изучение программной реализации методов цифровой стеганографии.

3.2 Самостоятельная работа обучающегося

Таблица 3.3

№	Виды самостоятельной работы	Индикаторы достижения компетенций	Часы на выполнение	Часы на консультации
Семестр: 2				
1	Подготовка к занятиям	ПК-3.В/НА.2,УК-2.1	43	3
Подготовка к лабораторным работам., подробная информация приведена в приложениях №1 №2 : Игнатьев, Е. Б. Основы криптографии : учебное пособие / Е. Б. Игнатьев. — Иваново : ИГЭУ, 2020. — 88 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154559 (дата обращения: 06.06.2022). — Режим доступа: для авториз. пользователей. Панкратова, И. А. Булевы функции в криптографии : учебное пособие / И. А. Панкратова. — Санкт-Петербург : Лань, 2022. — 92 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206174 (дата обращения: 06.06.2022). — Режим доступа: для авториз. пользователей.			
2	Подготовка к аттестации	ПК-3.В/НА.2,УК-2.1	30	2

Изучение конспекта лекций.: Игнатьев, Е. Б. Основы криптографии : учебное пособие / Е. Б. Игнатьев. — Иваново : ИГЭУ, 2020. — 88 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154559 (дата обращения: 06.06.2022). — Режим доступа: для авториз. пользователей. Панкратова, И. А. Булевы функции в криптографии : учебное пособие / И. А. Панкратова. — Санкт-Петербург : Лань, 2022. — 92 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206174 (дата обращения: 06.06.2022). — Режим доступа: для авториз. пользователей.

3.3 Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 3.4).

Таблица 3.4

Деятельность	Информационно-коммуникационные технологии
Информирование	e-mail; Среда электронного обучения НГТУ
Консультирование	e-mail; Среда электронного обучения НГТУ
Контроль	e-mail; Среда электронного обучения НГТУ
Размещение учебных материалов	Среда электронного обучения НГТУ; ЭБС

Таблица 3.5

Активные и интерактивные формы проведения занятий

№	Наименование активных форм
1	Дискуссия
Краткое описание применения:	

4. Правила аттестации обучающихся по дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 4.1.

Таблица 4.1

Оцениваемые виды деятельности обучающихся	Мин. балл	Максимальный балл
Семестр: 2		
Лабораторная:	30	60
Зачет:	20	40
Контролирующие материалы (список вопросов) приводятся в "Панкратова, И. А. Булевы функции в криптографии : учебное пособие / И. А. Панкратова. — Санкт-Петербург : Лань, 2022. — 92 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206174 (дата обращения: 06.06.2022). — Режим доступа: для авториз. пользователей."		

В таблице 4.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 4.2

Коды компетенций	Индикаторы достижения компетенций	Формы контроля
ПК-3.В/НА	ПК-3.В/НА 2. Умеет применять современные технологии обработки информации, компьютерных сетей и телекоммуникаций	
УК-2	УК-2 1. Знает особенности управления проектом в зависимости от этапа жизненного цикла	

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

5. Литература

Основная литература

1. Информационный мир XXI века. Криптография — основа информационной безопасности : методическое руководство / под ред. Э. А. Болелова ; Московский государственный технический университет гражданской авиации. - 4-е изд. — Москва : Издательско-торговая корпорация «Дашков и К°», 2020. — 126 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1081675 (дата обращения: 06.06.2022). – Режим доступа: по подписке.

2. Криптографическая защита информации : учебное пособие / С. О. Крамаров, О. Ю. Митясова, С. В. Соколов [и др.] ; под ред. С. О. Крамарова. — Москва : РИОР : ИНФРА-М, 2021. — 321 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1153156 (дата обращения: 06.06.2022). – Режим доступа: по подписке.

3. Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. - Красноярск : Сиб. федер. ун-т, 2019. - 206 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1819309 (дата обращения: 06.06.2022). – Режим доступа: по подписке.

4. Баранова, Е. К. Основы информатики и защиты информации: Учебное пособие / Баранова Е.К. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 183 с. (Высшее образование: Бакалавриат). - Текст : электронный. - URL: https://znanium.com/catalog/product/959916 (дата обращения: 06.06.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Романов Е. Л. Программная инженерия : [учебное пособие] / Е. Л. Романов.- Новосибирск, 2017.- 393, [1] с. : ил., табл..- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000238285

2. Котов Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т.- Новосибирск, 2016.- 57, [1] с..- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232326

Интернет-ресурсы

1. Znanium.com : электронно-библиотечная система : сайт. – Москва, 2011– . – URL: http://znanium.com/ (дата обращения: 02.03.2022). – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

6. Методическое и программное обеспечение, информационные технологии

6.1 Методическое обеспечение

1. Игнатьев, Е. Б. Основы криптографии : учебное пособие / Е. Б. Игнатьев. — Иваново : ИГЭУ, 2020. — 88 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154559 (дата обращения: 06.06.2022). — Режим доступа: для авториз. пользователей.

2. Панкратова, И. А. Булевы функции в криптографии : учебное пособие / И. А. Панкратова. — Санкт-Петербург : Лань, 2022. — 92 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206174 (дата обращения: 06.06.2022). — Режим доступа: для авториз. пользователей.

6.2 Специализированное программное обеспечение

1 ОС для применения на серверах Microsoft Windows

6.3 Информационные технологии

При осуществлении образовательного процесса по дисциплине применяются элементы дистанционных образовательных технологий, а также синхронного и асинхронного взаимодействия в электронной информационно-образовательной среды НГТУ.

7. Материально-техническое обеспечение

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Компьютеры объединены в локальную сеть с выходом в Internet