

Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Донецкий государственный университет»

Факультет математики и информационных технологий
Кафедра информационных систем управления

УТВЕРЖДАЮ
проректор

_____ П. А. Машаров
«17» апреля 2025 г.
МП

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Укрупненная группа направлений подготовки	46.00.00 История и археология
Программа высшего образования	Программа бакалавриата
Направление подготовки	46.03.02 Документоведение и архивоведение
Направленность (профиль) образовательной программы	Документоведение и архивоведение
Квалификация	Бакалавр
Форма обучения	Очная, очно-заочная

Рабочая программа может быть адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2025

Рабочая программа дисциплины **«Информационная безопасность и защита информации»** для обучающихся по направлению подготовки 46.03.02 Документоведение и архивоведение (Профиль: Документоведение и архивоведение) составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 46.03.02 Документоведение и архивоведение, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 29 октября 2020 г. № 1343 (с изм. и доп.), Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2025 года.

Разработчик:

доцент кафедры информационных систем
управления, канд. экон. наук, доцент

А. М. Гизатулин

Рабочая программа одобрена на заседании кафедры информационных систем
управления.

Протокол от 14.04.2025 г. № 13.

Заведующий кафедрой

Н.Ш. Пономаренко

СОГЛАСОВАНО:

Декан факультета математики и
информационных технологий
16.04.2025 г.

И. А. Моисеенко

Учебно-методическая комиссия факультета математики и информационных технологий.

Протокол от 16.04.2025 г. № 3.

Председатель

Л. И. Селякова

Руководитель основной образовательной
программы, д-р экон. наук, доц.
14.04.2025 г.

Н.Ш. Пономаренко

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:

Информационные технологии в документационном обеспечении управления и архивном деле, Информационные технологии и инструменты программирования, (сопутствующими дисциплинами – Системный анализ информационных процессов).

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее:

Информационная безопасность и защита информации; Производственная практика: проектная практика по архивоведению; Производственная практика: преддипломная; Подготовка к процедуре защиты и защита выпускной квалификационной работы.

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	46.03.02 Документоведение и архивоведение (Профиль подготовки: Документоведение и архивоведение)
Шифр и название в соответствии с учебным планом	Б1.В.ОД.2. Информационная безопасность и защита информации
Часть образовательной программы	Вариативная часть: выбор вуза
Количество зачетных единиц / всего часов	4 / 144

2.2. Распределение часов по формам и периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная	4	7	34	–	34	76	144	экзамен
Очно-заочная	4	8	10	–	10	138	144	экзамен

3. ЦЕЛИ ДИСЦИПЛИНЫ

Цель дисциплины «Информационная безопасность и защита информации» – формирование у будущего специалиста в сфере документоведения и архивоведения знаний, умений и навыков, позволяющих принимать решения в сфере информационной безопасности.

**4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ
ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ
И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ**

Компетенции	Индикаторы	Результаты обучения
ПК-6. Способен организовывать сопровождение цифровой трансформации документированных сфер деятельности организации	ПК-6.2. Демонстрирует способность разрабатывать политику информационной безопасности	ПК-6.2.1 Знает основы разработки политики информационной безопасности. ПК-6.2.2 Умеет разрабатывать документы «Политика информационной безопасности», «Специализированная политика (по областям применения)». ПК-6.2.3 Владеет приемами защиты информации в профессиональной деятельности.

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
Основные понятия и анализ угроз информационной безопасности	1.1. Основные понятия защиты информации и информационной безопасности 1.2. Анализ угроз информационной безопасности 1.3. Способы обеспечения безопасности информационных систем
Политика информационной безопасности	2.1 Политика информационной безопасности 2.2. Уровни политики безопасности 2.3. Структура политики безопасности организации 2.4. Базовая политика безопасности 2.5. Специализированные политики безопасности 2.6. Политика допустимого использования. 2.7. Политика удаленного доступа. 2.8. Процедуры безопасности 2.9. Процедура реагирования на события. 2.10. Процедура управления конфигурацией. 2.11. Разработка политики безопасности организации 2.12. Организация информационной безопасности банка
Криптографическая защита информации	3.1. Основные понятия криптографической защиты информации. 3.2. Классификация криптографических алгоритмов. 3.3. Электронная цифровая подпись. 3.4. Основные процедуры цифровой подписи. 3.5. Алгоритм цифровой подписи ГОСТ Р 34.10-94 3.6. Алгоритм цифровой подписи ECDSA. 3.7. Стандарт цифровой подписи ГОСТ Р 34.10-2001. 3.8. Управление криптоключами.
Идентификация, аутентификация и управление доступом	4.1. Аутентификация, авторизация и администрирование действий пользователей. 4.2. Аутентификация на основе многоразовых паролей. 4.3. Аутентификация на основе одноразовых паролей. 4.4. Идея строгой аутентификация. 4.5. Строгая двухфакторная аутентификация. 4.6. Применение смарт-карт. 4.7. Применение USB-токенов. 4.8. Особенности использования PIN-кода. 4.9. Криптографические протоколы строгой аутентификации.

	4.10. Биометрическая аутентификация пользователя. 4.11. Управление доступом по схеме однократного входа с авторизацией Single Sign-On. 4.12. Простая система однократного входа Single Sign-On. 4.13. Системы однократного входа Web SSO. 4.14. SSO-продукты уровня предприятия.
Защита электронного документооборота	5.1. Концепция электронного документооборота. 5.2. Особенности защиты электронного документооборота. 5.2.1. Угрозы для СЭД 5.2.2. Средства защиты СЭД 5.3. Защита баз данных 5.3.1. Основные типы угроз 5.3.2. Методы и средства защиты СУБД 5.3.3. Средства защиты СУБД Microsoft Access 5.3.4. Средства защиты СУБД Oracle 5.3.5. Защищенный доступ к базам данных 5.4. Защита корпоративного почтового документооборота 5.5. Защита системы электронного документооборота DIRECTUM 5.5.1. Функциональные возможности системы DIRECTUM 5.5.2. Архитектура системы DIRECTUM 5.5.3. Управление электронными документами в системе DIRECTUM

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – очная, курс – 4, семестр – 7

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Тема 1. Основные понятия и анализ угроз информационной безопасности	6	–	6	17	29
Тема 2. Политика информационной безопасности	8	–	8	13	29
Тема 3. Криптографическая защита информации	4	–	4	20	28
Тема 4. Идентификация, аутентификация и управление доступом	8	–	8	13	29
Тема 5. Защита электронного документооборота	8	–	8	13	29
ИТОГО ЗА СЕМЕСТР	34	–	34	76	144

6.2. Форма обучения – очно-заочная, курс – 4, семестр – 8

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Тема 1. Основные понятия и анализ угроз информационной безопасности	2	–	2	25	29
Тема 2. Политика информационной безопасности	2	–	2	25	29
Тема 3. Криптографическая защита информации	2	–	2	24	28
Тема 4. Идентификация, аутентификация и управление доступом	2	–	2	25	29

Тема 5. Защита электронного документооборота	2	–	2	25	29
ИТОГО ЗА СЕМЕСТР	10	–	10	124	144

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Контрольные вопросы

1. Сформулируйте понятие информационной безопасности ИС.
2. Объясните понятия целостности, конфиденциальности и доступности информации.
3. Объясните понятия идентификации, аутентификации и авторизации пользователя. Как они взаимосвязаны?
4. Укажите отличия санкционированного доступа от несанкционированного доступа к информации.
5. Сформулируйте определение политики безопасности.
6. Сформулируйте особенности избирательной и полномочной политики безопасности.
7. Объясните понятие «угроза безопасности ИС».
8. Укажите основные признаки классификации возможных угроз безопасности ИС.
9. Каковы основные виды угроз безопасности ИС по цели и степени воздействия?
10. Дайте краткую характеристику угроз безопасности, обозначаемых терминами: «троянский конь», «вирус», «червь»?
11. Перечислите и дайте краткую характеристику основных методов реализации угроз информационной безопасности.
12. Объясните суть комплексного подхода к обеспечению информационной безопасности ИС.
13. Объясните понятие «политика безопасности организации».
14. Какие разделы должна содержать документально оформленная политика безопасности?
15. Какие проблемы решает верхний уровень политики безопасности?
16. Какие задачи решает средний уровень политики безопасности?
17. Каковы особенности нижнего уровня политики безопасности?
18. Сформулируйте обязанности руководителей подразделений, администраторов и пользователей при реализации политики безопасности.
19. Опишите структуру политики безопасности организации.
20. Что представляют собой специализированные политики безопасности?
21. Приведите несколько примеров специализированных политик безопасности с описанием их особенностей.
22. Что представляют собой процедуры безопасности?
23. Приведите несколько примеров процедур безопасности с описанием их особенностей.
24. Сформулируйте основные этапы разработки политики безопасности организации.
25. Что такое криптография?
26. Дайте определения следующих понятий: криптограмма, криптоалгоритм, криптосистема.
27. В чем состоит коренное различие симметричных и асимметричных криптосистем?
28. Охарактеризуйте четыре основных режима работы блочного алгоритма.
29. Расскажите о способах комбинирования блочных алгоритмов для получения алгоритмов с более длинным ключом, сравните их между собой.

30. Каковы основные характеристики и режимы работы отечественного стандарта шифрования данных?
31. Сформулируйте концепцию криптосистемы с открытым ключом?
32. Дайте определение однонаправленной функции. Приведите примеры однонаправленных функций.
33. Каковы особенности однонаправленных функций с «потайным ходом»?
34. На чем основывается надежность криптоалгоритма шифрования RSA?
35. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности электронного документа.
36. Опишите отечественный стандарт цифровой подписи, укажите его преимущества по сравнению с алгоритмом цифровой подписи DSA.
37. Каково назначение хэш-функции и каким требованиям должна удовлетворять качественная хэш- функция?
38. Каким образом комбинированный метод шифрования позволяет сочетать достоинства асимметричных и симметричных криптосистем? Опишите протокол реализации комбинированного метода шифрования.
39. Опишите работу алгоритма Диффи - Хэлла. Укажите достоинства этого алгоритма.
40. Каково назначение инфраструктуры открытых ключей PKI? Опишите функционирование инфраструктуры PKI.
41. Дайте определения понятий: идентификация, аутентификация, авторизация, администрирование. Что понимают под решением задач AAA?
42. Какие задачи решает подсистема управления идентификацией и доступом IAM (Identity and Access Management)?
43. На какие категории можно разделить процессы аутентификации в зависимости от сущностей, предъявляемых пользователем для подтверждения своей подлинности?
44. Перечислите основные атаки на протоколы аутентификации.
45. Опишите метод аутентификации на основе многопарольных паролей. Каковы недостатки этого метода?
46. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки?
47. Сформулируйте принцип строгой аутентификации. Опишите типы процедур строгой аутентификации.
48. Объясните назначение PIN-кода и особенности его использования.
49. Объясните принцип работы двухфакторной аутентификации. Какие внешние носители информации используются для двухфакторной аутентификации пользователей? Каковы достоинства этого метода аутентификации?
50. Опишите функциональность и характеристики смарт-карт и USB-токенов.
51. Опишите методы биометрической аутентификации пользователя. Что означают коэффициент ошибочных отказов и коэффициент ошибочных подтверждений?
52. Поясните принцип управления доступом по схеме однократного входа с авторизацией Single Sign-On.
53. Укажите преимущества электронного документооборота по сравнению с бумажным документооборотом. Укажите различия между понятиями «система электронного документооборота» (СЭД) и ECM (Enterprise Content Management).
54. Охарактеризуйте базовые составляющие системы электронного документооборота.
55. Опишите функциональность подсистемы автоматизации управления потоками работ (Workflow).
56. Укажите особенности построения и функционирования системы распределенного электронного документооборота.

57. Назовите угрозы информационной безопасности для СЭД и охарактеризуйте источники этих угроз.
58. Какие функции должны быть реализованы средствами защиты информации СЭД?
59. Назовите основные угрозы информационной безопасности баз данных. Укажите методы и средства защиты СУБД.
60. Определите понятие «RAID-массив». Поясните особенности применения RAID-массивов в СУБД.
61. Сравните возможности средств защиты СУБД Microsoft Access и СУБД Oracle.
62. Охарактеризуйте методы и средства защиты корпоративного почтового документооборота.
63. Опишите функциональные возможности и архитектуру системы электронного документооборота DIRECTUM.
64. Охарактеризуйте приемы и методы защиты, реализованные в системе DIRECTUM.

7.2. Темы письменных работ (типы задач)

Практические работы по темам:

Тема 1. Основные понятия и анализ угроз информационной безопасности

Тема 2. Политика информационной безопасности

Тема 3. Криптографическая защита информации

Тема 4. Идентификация, аутентификация и управление доступом

Тема 5. Защита электронного документооборота.

7.3. Образец содержания экзаменационного билета

ФГБОУ ВО «ДОНЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Образовательная программа **бакалавриат**

Направление подготовки: **46.03.02 Документоведение и архивоведение**

Очная форма обучения. **Семестр VII**

Учебная дисциплина **Информационная безопасность и защита**

информации

БИЛЕТ № 1

1. Уровни политики безопасности.
2. Угрозы для системы электронного документооборота.

Утверждено на заседании кафедры информационных систем управления, протокол № от “___” сентября 2025 г.

Зав. кафедрой

Н. Ш. Пономаренко

Экзаменатор

А. М. Гизатулин

В случае ведения учебного процесса с использованием электронного обучения и дистанционных образовательных технологий, содержание билета может отличаться от приведенного.

8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-балльной шкале исходя из максимума, приведенного в таблице ниже.

Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение домашних заданий, активность во время проведения лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

Самостоятельная работа оценивается на основе предоставленных на проверку выполненных домашних, индивидуальных заданий с учетом своевременности их предоставления и соответствия требованиям к их выполнению.

Количество баллов за контрольную работу вычисляется как сумма баллов за все входящие в её состав задания. Каждое задание оценивается исходя из максимально возможного количества баллов с учетом правильности выполнения задания, полноты приводимых обоснований.

По результатам работы в семестре обучающийся, набравший не менее 60 баллов, имеет право получить оценку. Те, кто претендует на более высокий балл, проходят промежуточную аттестацию. Максимальное количество баллов на промежуточной аттестации – 100. Общее количество баллов за семестр вычисляется как максимальная из полученных за семестр и на промежуточной аттестации и выставляется согласно принятому порядку.

8.1. Семестр 1

Номера разделов	Виды работ	Максимальное количество баллов
1	Организационно-учебная работа в аудитории	10
	Самостоятельная работа (выполнение практических работ по варианту)	80
	Контрольная работа по теоретическому материалу	10
ИТОГО		100
Промежуточная аттестация		100
Общий итог за семестр		100

Соответствие баллов оценке

Количество баллов из 100	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет
90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено
70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в в 8-м учебном корпусе (г. Донецк, ул. Челюскинцев, д. 198 а) университета. Для проведения лабораторных занятий требуется аудитория,

оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя, выход в Интернет – проводной или с использованием Wi-Fi.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, учебно-методическое обеспечение, представленное в учебно-методическом кабинете Главного корпуса (ауд.405).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». При изучении дисциплины применяются электронное обучение и дистанционные образовательные технологии.

С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

10. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

10.1. Основная литература

1. Бондаренко, И. С. Информационная безопасность : учебник / И. С. Бондаренко. — Москва : МИСИС, 2023. — 254 с.
2. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с.
3. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 324 с.

10.2. Дополнительная литература

1. Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с.

11. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. **Национальная электронная библиотека (НЭБ):** федеральная государственная информационная система / Министерство Культуры РФ; Российская государственная библиотека. — Москва, 2019- . — URL: <https://rusneb.ru/> (дата обращения: 01.04.2025). — Режим доступа: свободный, подписка. Необходима установка программного обеспечения. — Текст: электронный.
2. **eLIBRARY.RU:** научная электронная библиотека: сайт. — Москва, 2000- . — URL: <https://elibrary.ru> (дата обращения: 01.04.2025). — Режим доступа: для авторизов. пользователей. — Текст: электронный.
3. Научная электронная библиотека **«КиберЛенинка»:** сайт / Ассоциация «Открытая наука». — Москва, 2014- . — URL: <https://cyberleninka.ru/>. — Режим доступа: свободный. — Текст: электронный.
4. Электронно-библиотечная система **«Лань»:** [сайт]. — URL: <https://e.lanbook.com> (дата обращения: 01.04.2025). — Режим доступа: для авторизов. пользователей. — Текст: электронный.
5. **ЭБС Юрайт:** электронная библиотечная система: сайт. — Москва, 2013. — URL: <https://biblio-online.ru> (дата обращения: 01.04.2025). — Режим доступа: для авторизов. пользователей. — Текст: электронный.
6. **Электронно-библиотечная система ДонГУ:** сайт / ФГБОУ ВО «ДонГУ». — Донецк, 2016- . — URL: <http://library.donnu.ru/> (дата обращения: 01.04.2025). — Режим доступа: свободный. — Текст: электронный.

7. **Электронный каталог** Научной библиотеки ДонГУ: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://library.donnu.ru/catalog/> (дата обращения: 01.04.2025). – Режим доступа: поиск свободный, электронные документы – для пользователей ДонГУ.

8. **Электронный архив ДонГУ**: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://repo.donnu.ru/> (дата обращения: 01.04.2025). – Режим доступа: свободный.

12. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Microsoft Visual Studio (лицензия программы Dream Spark для высших учебных заведений)
4. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения).