

Федеральное государственное образовательное бюджетное учреждение
высшего образования
**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**
(Финуниверситет)

Тульский филиал Финуниверситета

Кафедра «Математика и информатика»

УТВЕРЖДАЮ



Директор Тульского филиала

Г.В. Кузнецов

26 мая 2026 г.

Приложение к рабочей программе дисциплины

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Направление подготовки 38.03.05 – Бизнес-информатика,
образовательная программа «Цифровая трансформация управления бизнесом»,
Профиль: ИТ-менеджмент в бизнесе

Фамилия И.О. научно-педагогического работника филиала, ответственного за
актуализацию РПД Г.В. Ваныкина

Год утверждения рабочей программы дисциплины – 2025

*Одобрено кафедрой «Математика и информатика»
Протокол от 05 мая 2026 г. № 11*

Тула 2026

СОДЕРЖАНИЕ

Разделы рабочей программы с внесенными изменениями

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы	3
4. Объем дисциплины в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	3
5.2. Учебно-тематический план	4
5.3 Содержание семинаров, практических занятий	4
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	5
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	5
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	6
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	7
7.1. Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний	7
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	9
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	11
10. Методические указания для обучающихся по освоению дисциплины	11
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	12
11.1. Комплект лицензионного программного обеспечения	12
11.2. Современные профессиональные базы данных и информационные справочные системы	12
11.3. Сертифицированные программные и аппаратные средства защиты информации	12
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	13

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Дисциплина «Управление информационной безопасностью» обеспечивает формирование следующих компетенций:

Таблица 1

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
ПКН-4	Способность создавать модели архитектуры предприятия	1. Разрабатывает модели архитектуры предприятия.	Знать принципы и современные методологии разработки моделей архитектуры предприятия с учетом требований информационной безопасности; Уметь разрабатывать модели архитектуры предприятия с учетом требований информационной безопасности.
		2. Консультирует по вопросам применения архитектурного подхода, выбора структуры и языка моделирования архитектуры предприятия.	Знать особенности применения архитектурного подхода к управлению компанией с учетом требований информационной безопасности; Уметь использовать архитектурный подход к управлению компанией с учетом требований информационной безопасности.

4. Объем дисциплины в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Таблица 2

Вид учебной работы по дисциплине	Всего (в з/ед. и часах)	Семестр 2 (в часах)
Общая трудоемкость дисциплины	4 зач.ед. / 144 ч.	144
Контактная работа - Аудиторные занятия	50	50
<i>Лекции</i>	16	16
<i>Семинары, практические занятия</i>	34	34
Самостоятельная работа	94	94
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	зачет	зачет

5.2. Учебно-тематический план

Таблица 3

№ п/п	Наименование темы (раздела) дисциплины	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего	Контактная работа – Аудиторная работа			Самостоя тельная работа	
			Общая	Лекции	Семинары, практические занятия		
1	Общие вопросы управления ИБ организации	32	12	4	8	20	Доклады, презентации, дискуссии
2	Специальные вопросы управления ИБ организации	38	12	4	8	26	Доклады, презентации, дискуссии
3	Реализация системы управления ИБ организации	38	12	4	8	26	Доклады, презентации, дискуссии
4	Внутренние нормативные документы по управлению ИБ организации	36	14	4	10	22	Доклады, презентации, дискуссии
	В целом по дисциплине	144	50	16	34	94	Согласно учебному плану: контрольная работа
Итого:		100	38	32	68	62	

5.3 Содержание семинаров, практических занятий

Таблица 4

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)	Формы проведения занятий
Общие вопросы управления ИБ организации	Роль стандартов в управлении ИБ. Основные организации, издающие стандарты по вопросам управления ИБ. Комплекс стандартов и рекомендаций Банка России по управлению ИБ. Общие требования к системам менеджмента ИБ. Рекомендуемые источники: 8, 1-2	Групповые дискуссии, презентация основных подходов.
Специальные вопросы управления ИБ организации	Управление информационной безопасностью финансовых организаций. Требования и рекомендации Банка России и других регуляторов в сфере управления ИБ финансовых организаций. Комплекс СТО и РС БР ИББС. ГОСТ Р 57580.1 и 57580.2. Вопросы ИБ индустрии платежных карт.	Групповые дискуссии, презентация основных подходов

	Отдельные направления менеджмента ИБ. Обеспечение непрерывности деятельности и восстановления после прерываний. Рекомендуемые источники: 8, 1-2	
Реализация системы управления ИБ организации	Планирование в управлении ИБ. Внедрение системы управления ИБ. Анализ системы управления ИБ. Совершенствование системы управления ИБ организации. Рекомендуемые источники: 8, 1-2	Групповые дискуссии, презентация основных подходов
Внутренние нормативные документы по управлению ИБ организации	Иерархия внутренних нормативных документов по управлению информационной безопасностью. Требования к организации документационного обеспечения управления информационной безопасностью. Политика информационной безопасности организации. Другие документы по управлению ИБ. Рекомендуемые источники: 8, 1-2	Групповые дискуссии, презентация основных подходов

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Таблица 5

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Общие вопросы управления ИБ организации	Стандарты систем менеджмента качества в управлении ИБ	Работа с учебной литературой. Подготовка сообщений по теме; подготовка презентаций по теме.
Специальные вопросы управления ИБ организации	Положения ГОСТ Р 57580.1 в документах Банка России. Менеджмент инцидентов ИБ. Обеспечение непрерывности деятельности и восстановления после прерываний.	Работа с учебной литературой. Подготовка сообщений по теме; подготовка презентаций по теме.
Реализация системы управления ИБ организации	Определение подхода к оценке риска в организации. Управление ресурсами системы управления ИБ организации. Измерение результативности мер управления для проверки соответствия требованиям ИБ.	Работа с учебной литературой. Подготовка сообщений по теме; подготовка презентаций по теме.
Внутренние нормативные документы по управлению ИБ организации	Частные политики ИБ, их назначение и состав.	Работа с учебной литературой. Подготовка сообщений по теме; подготовка презентаций по теме.

6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю

Текущий контроль осуществляется в ходе учебного процесса и контроля самостоятельной работы студентов, в том числе по результатам выполнения контрольной работы. Основными формами текущего контроля знаний являются:

- обсуждение вопросов и задач, вынесенных в планах практических занятий в качестве самостоятельных заданий;
- обсуждение подготовленных презентаций;
- выполнение контрольной работы и обсуждение результатов.

Примерный перечень вопросов для дискуссий

1. Национальная платежная система, ее участники и требования к обеспечению ИБ.
2. Менеджмент инцидентов ИБ.
3. Управление в инфраструктуре открытых ключей.
4. Мошеннические операции в кредитно-финансовой сфере.
5. Аудит ИБ.

Примерный перечень тем докладов с презентациями

1. Международные и национальные российские стандарты по информационной безопасности.
2. Международные и национальные российские стандарты по управлению информационной безопасностью.
3. Регулирование ИБ международных карточных платежных систем.
4. Требования к обеспечению ИБ в РФ.
5. Требования к обеспечению ИБ в финансовых организациях РФ.

Примерные задания контрольной работы:

1. Виды информации, подлежащей защите в РФ.
2. Оценка соответствия требованиям ИБ в КФО.
3. Профили защиты.
4. Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций
5. Ключевые требования к защите информации при осуществлении переводов денежных средств.
6. Методика оценки модели угроз и ее применение.
7. Ключевые субъекты НПС.

Критерии балльной оценки различных форм текущего контроля успеваемости

Организация текущего контроля успеваемости обучающихся по итогам семестра (модуля), по программам бакалавриата и магистратуры в соответствии с учебными планами по направлениям подготовки высшего образования утверждена приказом ректора Финуниверситета по основной деятельности от 23.03.2017 №0557/о «Об утверждении Положения о проведении текущего

контроля успеваемости и промежуточной аттестации обучающихся по программам бакалавриата и магистратуры в Финансовом университете».

Таблица 6 - Виды работ обучающегося, формирующие текущий контроль по дисциплине

Вид учебной деятельности	Баллы	Максимум за семестр (модуль)
Выполнение и защита контрольной работы	10	10
Аудиторная контрольная/срезовая работа	5	10
Тестирование/блиц опросы	0,2	10
Посещение занятий, ведение конспекта лекции/семинара и работа с ним	0,1	4
Активное участие в интерактивном процессе выполнения практических заданий на семинарском занятии	0,1	6
Всего за семестр (модуль)	40	

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине содержится в разделе «2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».

7.1. Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний

Таблица 7

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые задания
ПКН-4 Способность создавать модели архитектуры предприятия	Индикатор 1. Разрабатывает модели архитектуры предприятия	Знать принципы и современные методологии разработки моделей архитектуры предприятия с учетом требований информационной безопасности. Уметь разрабатывать модели архитектуры предприятия с учетом требований	Задание 1. Составить план контроля соблюдения требований информационной безопасности на рабочем месте. Задание 2. Составить план проведения тренировок по повышению соблюдения требований информационной безопасности.

		информационной безопасности.	
	Индикатор 2. Консультирует по вопросам применения архитектурного подхода, выбора структуры и языка моделирования архитектуры предприятия	Знать особенности применения архитектурного подхода к управлению компанией с учетом требований информационной безопасности. Уметь использовать архитектурный подход к управлению компанией с учетом требований информационной безопасности.	Задание 1. Составить аналитический обзор инфраструктурных решений центров обработки данных. Задание 2. Изложить варианты сегментации вычислительного оборудования центров обработки данных согласно требованиям к защите информации финансовых организаций.

Примерный перечень вопросов для подготовки к зачету

1. Какие действия и процессы составляют стадию проверки СУИБ?
2. В чем состоит обеспечение информационной безопасности автоматизированных систем на стадии разработки технических заданий?
3. Что такое информационная безопасность, информационная безопасность объекта информатизации, безопасность информации, безопасность информационной технологии, киберустойчивость (в финансовой сфере)?
4. В чем состоит обеспечение информационной безопасности автоматизированных систем на стадии проектирования?
5. Что такое система менеджмента организации и система менеджмента информационной безопасности организации?
6. В чем заключается процессный подход к управлению ИБ?
7. На какие категории подразделяются персональные данные?
8. Что такое банковская тайна?
9. Какие вопросы защиты информации в негосударственной сфере регулирует ФСТЭК?
10. Что такое идентификация и аутентификация?
11. Какие действия и процессы составляют стадию планирования СУИБ?
12. Что такое угроза (безопасности информации), уязвимость (объекта защиты), риск ИБ?
13. Что такое циклическая модель PDCA применительно к управлению ИБ?
14. Что включает выбор и применение финансовой организацией мер ЗИ согласно ГОСТ Р 57580.1-2017?
15. В каких случаях, согласно ГОСТ Р 57580.1-2017, возможно использование компенсирующих мер ЗИ? Какие условия при этом должны быть выполнены?

16. Что такое контур безопасности и уровень защиты информации, согласно ГОСТ Р 57580.1-2017? Кем и на основании чего устанавливается уровень ЗИ финансовой организации для конкретного контура безопасности?

17. Укажите стадии жизненного цикла автоматизированных систем. Чем обусловлены особенности обеспечения информационной безопасности автоматизированных систем на различных стадиях жизненного цикла?

18. Назовите основные нормативно правовые документы в области управления информационной безопасности.

19. Какие вопросы защиты информации в негосударственной сфере регулирует ФСБ?

20. Какие виды информации подлежат защите в соответствии с нормативными актами госрегуляторов?

21. Укажите типы факторов аутентификации.

22. Опишите основные угрозы аутентификации.

23. Укажите плюсы и минусы парольной аутентификации.

Примеры практико-ориентированных заданий

Задача 1. Составьте модель угроз нарушения информационной безопасности для автоматизированной банковской системы коммерческого банка.

Задача 2. Составьте проект классификатора инцидентов ИБ.

Задача 3. Переформулируйте требования стандарта PCI DSS в терминах стандарта ГОСТ Р 57580.1.

Задача 4. В ходе проведенной службой информационной безопасности банка проверки были выявлены учетные записи ранее уволенных сотрудников. Предложите способы недопущения таких событий при следующих проверках со стороны службы ИБ.

Задача 5. В корпоративной сети кредитной организации выявлено автоматизированное рабочее место, на котором не установлен антивирус. Опишите возможные риски информационной безопасности, которые могут возникнуть.

Задача 6. Составьте развернутый план частной политики менеджмента инцидентов ИБ.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Нормативные акты

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (В редакции от 02.07.2021 г.).

2. Федеральный закон от 06 октября 1997 г. N 131-ФЗ «О государственной тайне» (В редакции от 11.06.2021 г.)

3. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (В редакции от 09.03.2021 г.).

4. Распоряжение Правительства России от 28 июля 2017 г. №1632-р «Об утверждении Программы «Цифровая экономика Российской Федерации»

5. Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

6. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

7. ГОСТ Р 50922 Защита информации. Основные термины и определения.

8. ГОСТ Р 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

9. ГОСТ Р 51583 Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.

10. ГОСТ Р 57628 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.

11. ГОСТ Р ИСО/МЭК 15408-1 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

12. ГОСТ Р ИСО/МЭК 15408-2 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.

13. ГОСТ Р ИСО/МЭК 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

14. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.

15. ГОСТ Р ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

16. ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

17. ГОСТ Р ИСО/МЭК ТО 19791 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

Основная литература

1. Гришина, Н. В. Основы информационной безопасности предприятия: учебное пособие / Н. В. Гришина. Москва : ИНФРА-М, 2024. 216 с. ЭБС ZNANIUM. URL: <https://znanium.com/catalog/product/2131865> (дата обращения : 12.01.2025). Текст : электронный.

2. Защита информации: учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин [и др.]. 3-е изд. Москва : РИОР : ИНФРА-М, 2024. 400 с. ЭБС

ZNANIUM. URL: <https://znanium.com/catalog/product/2140566> (дата обращения : 12.01.2025). Текст : электронный.

Дополнительная литература

Глинская Е. В., Чичварин Н. В. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]: учебное пособие. М.: ИНФРА-М, 2021. 118 с. <https://znanium.com/catalog/product/1178153> (дата обращения: 12.01.2025). Текст : электронный.

Мельников В.П., Куприянов А.И., Васильева Т.Ю. Информационная безопасность [Электронный ресурс]: учебник. М.: КноРус, 2022. 371 с. <https://book.ru/book/941809> (дата обращения: 05.05.2025). Текст : электронный.

Сычев Ю. Н. Защита информации и информационная безопасность [Электронный ресурс]: учебное пособие. М.: ИНФРА-М, 2021. 201 с. <https://znanium.com/catalog/product/1013711> (дата обращения: 12.01.2025). Текст : электронный.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Сайт Департамента анализа данных и машинного обучения Финансового университета.
2. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>
3. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
4. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>
5. Электронно-библиотечная система Znanium <http://www.znanium.com>
6. Электронно-библиотечная система издательства «ЮРАЙТ» <https://www.urait.ru/>
7. Электронно-библиотечная система издательства «Лань» <https://e.lanbook.com/>
8. Деловая онлайн-библиотека Alpina Digital <http://lib.alpinadigital.ru/>
9. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
10. Национальная электронная библиотека <http://нэб.рф/>

10. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студента в процессе освоения дисциплины включает в себя:

- подготовку к семинарским занятиям;
- изучение основной и дополнительной литературы по дисциплине;
- выполнение контрольной работы;
- индивидуальные или групповые консультации по наиболее сложным вопросам;
- подготовку к зачету.

Требования к оформлению контрольной работы

Контрольная работа является одной из форм самостоятельной работы студентов. Целью выполнения контрольной работы является подготовка студента к творческой деятельности научного или практического характера и формирование навыков представления полученных результатов.

Контрольная работа может выполняться как индивидуально, так и в составе группы.

Контрольная работа должна включать:

- описание цели и задач работы;
- круг рассматриваемых проблем и методы их решения;
- статистические данные с указанием источника информации;
- результаты анализа статистических данных и их интерпретация;
- общие выводы.

Оформление контрольных работ и домашнего творческого задания

Контрольные работы и домашнее творческое задание выполняются на листах А4. Оформляется титульный лист, выполненная работа с титульным листом в назначенный день сдается на проверку преподавателю.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем

11.1. Комплект лицензионного программного обеспечения

лицензионное отечественное:

1. Антивирусная защита Kaspersky Endpoint Security.
2. Astra Linux.
3. LibreOffice.

лицензионное импортное:

ПО для ТСО лиц с ограниченными возможностями здоровья

свободно распространяемое:

Архиватор KDE (Ark).

11.2. Современные профессиональные базы данных и информационные справочные системы

1. Информационно-правовая система «Гарант»
2. Информационно-правовая система «Консультант Плюс»
3. Информационно-образовательный портал Финансового университета:
<http://org.fa.ru>.

11.3. Сертифицированные программные и аппаратные средства защиты информации

Не используются.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Образовательный процесс по учебной дисциплине осуществляется в учебных аудиториях для проведения учебных занятий. При освоении дисциплины используются технические средства мультимедийной техники аудиторий.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения в сети «Интернет» и обеспечением доступа в электронно-образовательную среду Финансового университета.