

Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
Омский филиал Финуниверситета
Кафедра «Естественно-научные и гуманитарные дисциплины»

УТВЕРЖДАЮ
Директор Омского филиала
Финуниверситета

О.Р. Онищенко
«23» июня 2026 г.

ПРИЛОЖЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Год утверждения программы: 2025

Разработчики рабочей программы дисциплины: Велигура А.Н.

НАПРАВЛЕНИЕ **ПОДГОТОВКИ:** 38.03.05 «Бизнес-информатика»,
Образовательная программа «Цифровая
трансформация управления бизнесом: ИТ-
менеджмент в бизнесе»

Составитель актуализации: Лукина О.В.

*Рекомендовано Ученым советом Омского филиала Финуниверситета
(протокол от «23» июня 2026 г. №34)*

*Одобрено кафедрой «Естественно-научные и гуманитарные дисциплины»
(протокол от «29» апреля 2026 г. №4)*

Омск 2026

Приложение к программе дисциплины разработал: кандидат
технических наук, доцент ***О.В. Лукина***

Управление информационной безопасностью. Приложение к рабочей
программе дисциплины для студентов, обучающихся по направлению
подготовки 38.03.05 «Бизнес-информатика». – Омск, 2026. - 14 стр.

СОДЕРЖАНИЕ

4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	4
5.2. Учебно-тематический план	4
5.3. Содержание семинаров, практических занятий	5
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	6
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	6
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	7
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	7
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	11
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	12
10. Методические указания для обучающихся по освоению дисциплины	13
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	13
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	14

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

Трудоемкость дисциплины составляет 4 зачетные единицы. Виды учебной работы (в часах) представлены в таблице.

Вид учебной работы	Всего	Семестр 2
Общая трудоемкость дисциплины	144 (4 з.е.)	144
<i>Аудиторные занятия</i>	50	50
лекции	16	16
практические или семинарские занятия	34	34
<i>Самостоятельная работа</i>	94	94
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	зачет	зачет

5.2 Учебно-тематический план

№ п/п	Название темы (раздела) дисциплины	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего	Аудиторная работа			Самостоятельная работа	
			Общая	Лекции и	Практические занятия		
1	Общие вопросы управления ИБ организации	36	8	4	4	28	Аудиторная работа на семинарских занятиях, доклад, презентация Участие в дискуссии
2	Специальные вопросы управления ИБ организации	36	14	4	10	22	

3	Реализация системы управления ИБ организации.	36	14	4	10	22	
4	Внутренние нормативные документы по управлению ИБ организации.	36	14	4	10	22	
	Итого:	144	50	16	34	94	
					68%		

5.3. Содержание практических и семинарских занятий

№ п/п	Наименование темы (раздела) дисциплины	содержание практического занятия	Вопросы к практическому занятию
1	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. <i>Рекомендуемая литература:</i> 8:1-7; 9-12;9	Групповые дискуссии презентация основных подходов. Учебное задание: сравнение подходов к управлению ИБ ISO, России, США и Германии.
2	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 РСБР ИББС. ГОСТ Р 57580.1 и 57580.2. Вопросы ИБ индустрии платежных карт. Отдельные направления менеджмента ИБ. Обеспечение непрерывности деятельности и восстановления после прерываний. <i>Рекомендуемая литература:</i> 8:1-7; 9-12;9	Групповые дискуссии презентация основных подходов. Учебное задание: Исследование методики ГОСТ Р 57580.2
3	Реализация системы управления ИБ организации.	Планирование в управлении ИБ. Внедрение системы управления ИБ. Анализ системы управления ИБ. Совершенствование системы управления ИБ организации. <i>Рекомендуемая литература:</i> 8: 9-12;9	Групповые дискуссии презентация основных подходов. Учебное задание: Исследование методики оценки модели угроз

4	Внутренние нормативные документы по управлению информационной безопасности 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. Изучение примеров работы с форматами CSV, XML, XHTML, HTML, JSON при помощи Библиотек на языке Python, проектирование собственного приложения, работающего с одним из данных форматов. <i>Рекомендуемая литература: 8:1-7; 9-12;9</i>	групповые дискуссии презентация основных подходов. Учебное задание: Пример составления частных политик
---	---	---	--

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

6.1. Формы внеаудиторной самостоятельной работы

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, научной и справочной литературой; конспект; подготовка сообщений по теме; подготовка презентаций по теме; выполнение учебного задания
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, научной и справочной литературой; конспект; подготовка сообщений по теме; подготовка презентаций по теме; выполнение учебного задания
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, научной и справочной литературой; конспект; подготовка сообщений по теме; подготовка презентаций по теме; выполнение учебного задания

Внутренние нормативные документы по управлению ИБ организации.	Частные политики ИБ, их назначение и состав.	- работа с учебной, научной и справочной литературой; конспект; подготовка сообщений по теме; подготовка презентаций по теме; выполнение учебного задания
--	--	---

6.1. Методическое обеспечение для аудиторной и внеаудиторной самостоятельной работы

Пример варианта самостоятельной работы

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.

Примерные темы контрольных работ.

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 не кредитных 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.

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».

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

Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
УК-7 Способность создавать и поддерживать безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий и военных конфликтов	1. Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда.	Знать: - основные требования к технике безопасности на рабочем месте, безопасным условиям труда. Уметь: - выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда	Задание 1. Составить план контроля соблюдения техники безопасности на рабочем месте. Задание 2. Провести анализ возможных угроз на объекте, предложить меры физической защиты информации.
	2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	Знать: - основные мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах. Уметь: - проводить мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	Задание 1. Составить проект мероприятий по действиям в чрезвычайных ситуациях.
	3. Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества.	Знать: - основные проблемные ситуации, связанные с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества. Уметь: - находить пути решения	Задание 1. Составить план проведения тренировок по действиям в чрезвычайных ситуациях. Задание 2. Провести анализ проблемной ситуации, связанной с безопасностью жизнедеятельности людей на объекте,

Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества.	предложить пути решения ситуации.
	4. Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания	Знать: - основные способы выживания в экстремальных и чрезвычайных ситуациях. Уметь: - применять на практике основные способы выживания.	Задание 1 Составить проект методических рекомендаций по применению на практике основных способов выживания.
ПКН-12 Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных	Индикатор 1. Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знать: - способы анализа рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных. Уметь: - проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Задание 1 Составить аналитический обзор инфраструктурных решений центров обработки данных.
	Индикатор 2. Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знать: - основные варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных. Уметь: - формулировать предложения по использованию вычислительного	Задание 1 Изложить варианты сегментации вычислительного оборудования центров обработки данных согласно требованиям к защите информации финансовых организаций.

Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		оборудование, систем хранения данных и инфраструктурных решений центров обработки данных.	

Примерные вопросы к зачету:

1. В чем основное отличие информационной безопасности от киберустойчивости?
2. Укажите основные государственные органы, требования которых по защите информации обязательны.
3. Что такое угроза (ИБ)?
4. Что такое уязвимость (в контексте ИБ) и к чему она относится?
5. Какие виды информации подлежат защите в соответствии с нормативными актами госрегуляторов?
6. В чем заключаются особенности защиты коммерческой тайны?
7. Какие вопросы защиты информации регулирует ФСБ?
8. Какие виды информации подлежат защите в соответствии с нормативными актами госрегуляторов?
9. На какие категории подразделяются персональные данные?
10. Что такое банковская тайна?
11. Какие вопросы защиты информации регулирует ФСТЭК?
12. Что такое идентификация и аутентификация?
13. Перечислите технические и организационные средства/решения, которые помогают блокировать фишинговые атаки на уровне инфраструктуры и снижают риск успеха фишинга
14. Приведите примеры антивирусных программ.
15. Назовите основные нормативно-правовые документы в области управления информационной безопасностью.

16. Что такое циклическая модель PDCA применительно к управлению ИБ?
17. Какие виды информации подлежат защите в соответствии с нормативными актами госрегуляторов?
18. Что такое стеганография? Какими могут быть покрывающие сообщения?
19. Для чего нужна криптография, каковы основные принципы криптографии?
20. Поясните какие объекты относятся к критической информационной инфраструктуре (КИИ)?

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

Нормативные акты

1. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности».
2. Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».
3. Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе».
4. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
5. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
6. Федеральный закон от 06 октября 1997 г. N 131-ФЗ «О государственной тайне».
7. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне»
8. 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».
9. Письмо Банка России от 24 мая 2005 г. №76-Т «Об организации управления операционным риском в кредитных организациях».
10. Положение Банка России от 8 апреля 2020 г. № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»
11. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014.
12. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
13. ГОСТ Р 57580.1 – 2017. Безопасность финансовых (банковских) операций.

Защита информации финансовых организаций. Базовый состав организационных и технических мер.

14. ГОСТ Р 57580.2 – 2018. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия.

15. ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения»

16. ГОСТ Р 57580.4-2022 «Безопасность финансовых операций. Обеспечение (банковских) операционной надежности. Базовый состав организационных и технических мер»

17. ГОСТ Р ИСО ТО 13569-2007. Финансовые услуги. Рекомендации по информационной безопасности.

Основная литература:

18. 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 : 15.04.2026). — Текст : электронный.

19. 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 : 15.04.2026). - Текст : электронный.

Дополнительная литература:

20. Мельников, В. П. Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2025. — 267 с. — ISBN 978-5-406-13756-7. — URL: <https://book.ru/book/955528> (дата обращения: 15.04.2026). — Текст : электронный.

21. Милославская, Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд. – Москва : Горячая линия-Телеком, 2016. – 170 с. – ЭБС ZNANIUM. - URL: <https://znanium.com/catalog/product/560782> (дата обращения : 15.04.2026). – Текст : электронный.

22. Шилов, А. К. Управление информационной безопасностью: учебное пособие / А. К. Шилов; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. - 120 с. – ЭБС ZNANIUM. - URL: <https://znanium.com/catalog/product/1021744> (дата обращения : 15.04.2026). – Текст : электронный.

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

1. Сайт Центрального банка Российской Федерации: www.cbr.ru.

2. Сайт Федеральной службы по техническому и экспортному контролю:
www.fstec.ru.
3. Сайт Федерального агентства по техническому регулированию и метрологии:
www.gost.ru.
4. Электронная <http://elib.fa.ru/> библиотека Финансового университета (ЭБ)
5. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
6. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН»
<http://biblioclub.ru/>
7. Электронно-библиотечная система Znanium <http://www.znanium.com>
8. Электронно-библиотечная система издательства «ЮРАЙТ» <https://urait.ru/>
9. Электронно-библиотечная система издательства Проспект
<http://ebs.prospekt.org/books>
10. Электронно-библиотечная система издательства Лань <https://e.lanbook.com/>
11. Деловая онлайн-библиотека Alpina Digital <http://lib.alpinadigital.ru/>
12. Электронная библиотека Издательского дома «Гребенников»
<https://grebennikon.ru/>
13. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
14. Национальная электронная библиотека <http://нэб.рф/>

10. Методические указания для обучающихся по освоению дисциплины

Студентам необходимо: ознакомиться с содержанием рабочей программы дисциплины (далее - РПД), с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы. РПД, а также все методические разработки по данной дисциплине имеются на образовательном портале.

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:
 - Astra Linux Special Edition
- 11.2. Современные профессиональные базы данных и информационные справочные системы:
 - Справочная правовая система «КонсультантПлюс»
(<http://www.consultant.ru>).
 - Информационно-образовательный портал Финансового университета
<https://org.fa.ru>, <http://campus.fa.ru>
- 11.3. Сертифицированные программные и аппаратные средства защиты информации – не предусмотрено.

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

Для осуществления образовательного процесса по дисциплине необходимо использовать аудитории, оснащенные компьютером и проектором для демонстрации презентаций.