

Федеральное государственное образовательное бюджетное учреждение
высшего образования
**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**
(Финансовый университет)
Кафедра «Информационная безопасность»

Г. О. Крылов
«Кибербезопасность в сфере финансов»

Рабочая программа дисциплины
для подготовки магистров по направлению подготовки
38.04.08 «Финансы и кредит»

Направленность программы
«Финансы государственного сектора»

Москва, 2022

Федеральное государственное образовательное бюджетное учреждение
высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

(Финансовый университет)

Кафедра «Информационная безопасность»

УТВЕРЖДАЮ

Проректор по развитию
образовательных программ

_____ Е.А. Каменева

«25.10.2022 г.

Г. О. Крылов

«Кибербезопасность в сфере финансов»

Рабочая программа дисциплины
для подготовки магистров по направлению подготовки
38.04.08 «Финансы и кредит»

Направленность программы
«Финансы государственного сектора»

*Рекомендовано Ученым советом факультета
«Прикладной математики и информационных технологий»
(протокол от «15» октября 2022 г. №18)*

*Одобрено заседанием кафедры «Информационная безопасность»
(протокол от «26» сентября 2022 г. № 3)*

Москва, 2022

УДК 004.451(073)
ББК 32.973я73

Рецензент: к.т.н., Ларионова С.Л. – доцент кафедры «Информационная безопасность»

Г.О. Крылов «Кибербезопасность в сфере финансов». Рабочая программа дисциплины для подготовки магистров по направлению подготовки 38.04.08 «Финансы и кредит», направленность программы «Финансы государственного сектора».

– М.: Финансовый университет, кафедра «Информационная безопасность», 2022 – 18 с.

Рабочая программа дисциплины содержит требования к результатам освоения дисциплины, содержание дисциплины, тематику семинарских занятий и технологии их проведения, формы самостоятельной работы, контрольные вопросы и систему оценивания, учебно-методическое и информационное обеспечение дисциплины.

Учебное издание

Крылов Григорий Олегович
«Кибербезопасность в сфере финансов»

Рабочая программа дисциплины

Компьютерный набор, верстка Г.О. Крылов

Формат 60x90/16. Гарнитура *Times New Roman*
Усл. п.л. 1. Изд. № _____. – 2022. Тираж - 50 экз.

Заказ № _____

Отпечатано в Финансовом университете

© Г.О. Крылов, 2022

© Финансовый университет, 2022

СОДЕРЖАНИЕ

1. Наименование дисциплины.....	6
2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине	6
3. Место дисциплины в структуре образовательной программы.....	6
4. Объем дисциплины(модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	7
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	7
5.1. Содержание дисциплины.....	7
5.2. Учебно-тематический план	8
5.3. Содержание семинаров, практических занятий.....	9
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.....	10
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы.....	10
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	11
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.....	14
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	16
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.....	18
10. Методические указания для обучающихся по освоению дисциплины	19

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	19
11.1. Комплект лицензионного программного обеспечения	19
11.2. Современные профессиональные базы данных и информационные справочные системы	19
11.3. Сертифицированные программные и аппаратные средства защиты информации	19
12. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.....	20

1. Наименование дисциплины

«Кибербезопасность в сфере финансов»

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

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ПКН-2	Способность применять продвинутое современные инструменты и методы анализа финансово-кредитной сферы, финансов государственного и негосударственного секторов экономики для целей эффективного управления финансовыми ресурсами, решений проектно-экономических задач, в том числе, в условиях цифровой экономики и развития Финтех, разработки механизмов монетарного и финансового регулирования, как на уровне отдельных организаций и институтов финансового рынка, так и на уровне публично-правовых образований	<p>1. Владеет современными инструментами и методами анализа и регулирования финансов государственного и негосударственного секторов экономики, деятельности институтов финансово-кредитной сферы</p> <p>2. Демонстрирует способность решения проектно-экономических задач в профессиональной деятельности</p> <p>3. Демонстрирует освоение инструментов Финтех</p> <p>4. Владеет методами анализа Big Date, использует для решений профессиональных задач на</p>	<p>Знать принципы и методы обнаружения, идентификации и классификации уязвимостей, рисков и угроз нарушения информационной безопасности объектов кредитно-финансовой сферы; Уметь организовывать и проводить обнаружение, идентификацию и классификацию уязвимостей, рисков и угроз нарушения информационной безопасности объектов кредитно-финансовой сферы;</p> <p>Знать методы управления корпоративными рисками Уметь выстраивает систему управления корпоративными рисками</p> <p>Знать области применения инструментов Финтех Уметь формулировать предложения по созданию новых подходов для имеющихся решения задач в области Финтех</p> <p>Знать методы анализа Big Date Уметь использовать методы анализа Big Date для решения профессиональных задач на микро-, мезо- и макроуровнях, в том числе на уровне финансового рынка</p>

		микро-, мезо- и макроуровнях, в том числе на уровне финансового рынка	
--	--	---	--

3. Место дисциплины в структуре образовательной программы

Дисциплина «Кибербезопасность в сфере финансов» входит в модуль дисциплин по выбору углубляющих освоение образовательной программы магистратуры.

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

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Модуль 4 (в часах)
Общая трудоемкость дисциплины	3 з/е, 108 ч.	108
Контактная работа - Аудиторные занятия	16	16
<i>Лекции</i>	4	4
<i>Семинары, практические занятия</i>	12	12
Самостоятельная работа	92	92
<i>Вид текущего контроля</i>	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Зачет	Зачет

5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Задачи и основные направления деятельности Банка России в области информационной безопасности. Правовое регулирование. Обеспечение информационной безопасности и киберустойчивости инфраструктуры. Обеспечение информационной безопасности и киберустойчивости прикладного программного обеспечения. Обеспечение информационной безопасности и киберустойчивости технологий обработки данных. Обеспечение информационной безопасности и киберустойчивости финансовых технологий. Подготовка кадров и обеспечение доверия граждан к цифровой среде. Международное сотрудничество. Национальная программа «Цифровая экономика Российской Федерации». Центр компетенций по

обеспечению информационной безопасности и противодействию кибератакам в кредитно-финансовой сфере. Надзорная деятельность.

Тема 2. Конкурентная разведка и информационное противоборство в кредитно-финансовой сфере. Конкурентная разведка, цели и задачи. Методы выявления и анализа конкурирующих фирм. Понятие и содержание конкуренции в кредитно-финансовой сфере. Создание подразделений конкурентной разведки на предприятии. Интернет-разведка – как инструмент конкурентной разведки и модель угроз. Методы и приемы информационно-аналитической обработки информации о юридических и физических лицах. Информационное противоборство как система специальных мер обеспечения информационной безопасности.

Тема 3. Оценка защищенности кредитно-финансовых систем. Стандарты и методологии проверки и оценки защищенности ИТ и СУИБ: их отличия, сильные и слабые стороны. Международный стандарт оценки защищенности ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011. Базовые вопросы проверки защищенности. Оценка эффективности и результативности деятельности по управлению ИБ. Измерение, мера измерения, показатель и метрика. Метрики безопасности. Системы анализа защищенности.

Тема 4. Организация системы защиты информации кредитно-финансовых систем. Этапы построения системы защиты информации. Политика безопасности. Оценка эффективности инвестиций в информационную безопасность. Обеспечение компьютерной безопасности учетной информации. Обеспечение информационной безопасности автоматизированных банковских систем (АБС).

5.2. Учебно-тематический план

№ п/п	Наименование разделов дисциплины,	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего часов	Аудиторная работа			Самосто ятельна я работа	
			Общ ая	Лекц ии	Семинары, практичес кие занятия		
1.	Задачи Банка России в области информационной безопасности	27	3	1	2	24	Доклады, презентации и дискуссии

2.	Конкурентная разведка и информационное противоборство в кредитно-финансовой сфере.	29	5	1	4	24	Доклады, презентации и дискуссии
3.	Оценка защищенности кредитно-финансовых систем.	27	5	1	4	22	Доклады, презентации и дискуссии
4.	Организация системы защиты информации кредитно-финансовых систем	25	3	1	2	22	Доклады, презентации и дискуссии
	В целом по дисциплине	108	16	4	12	92	Согласно учебному плану: Контрольная работа

5.3. Содержание семинаров, практических занятий

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
Задачи Банка России в области информационной безопасности	Обеспечение информационной безопасности и киберустойчивости инфраструктуры. Обеспечение информационной безопасности и киберустойчивости прикладного программного обеспечения. Обеспечение информационной безопасности и киберустойчивости технологий обработки данных. Обеспечение информационной безопасности и киберустойчивости финансовых технологий. Источники: 8.1.; 8.3.;8.7.;8.11.;8.14.;8.15.	групповые дискуссии презентация основных подходов. Письменная работа <u>Учебное задание:</u> Практика оценки информационной обстановки и постановка задачи кибербезопасности
Конкурентная разведка и информационное противоборство в кредитно-финансовой сфере.	Информация, которая продается тайком. Чужой агент или человек с чужой визиткой. Работа с увольняемыми. Профилактика агентурной деятельности Конкурентная разведка в США. Конкурентная разведка во Франции. Финансовая разведка в России. Информационное противоборство как система мер обеспечения кибербезопасности.	групповые дискуссии презентация основных подходов. Письменная работа <u>Учебное задание:</u> Работа с увольняемыми.

	Источники: 8.1.;8.4.;8.7.;8.11.;8.12.;8.14.	
Оценка защищенности кредитно-финансовых систем.	Стандарты и методологии проверки и оценки защищенности ИТ и СУИБ: их отличия, сильные и слабые стороны. Международный стандарт оценки защищенности ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011. Базовые вопросы проверки защищенности. Оценка эффективности и результативности деятельности по управлению ИБ. Метрики безопасности. Системы анализа защищенности. Источники: 8.1.;8.3.;8.4.;8.12.;8.14.;8.16.	групповые дискуссии презентация основных подходов. <u>Учебное задание:</u> Определить причины отставания России в бенчмаркинге.
Организация системы защиты информации кредитно-финансовых систем	Этапы построения системы защиты информации. Политика безопасности. Оценка эффективности инвестиций в информационную безопасность. Обеспечение компьютерной безопасности учетной информации. Обеспечение информационной безопасности автоматизированных банковских систем (АБС). Источники: 8.1.;8.3.;8.7.;8.10.;8.11.;8.14.;8.15.	групповые дискуссии презентация основных подходов. Письменная работа <u>Учебное задание:</u> Контент-анализ выступления, интервью или беседы.

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

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

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Задачи Банка России в области информационной безопасности	Подготовка кадров и обеспечение доверия граждан к цифровой среде. Международное сотрудничество. Национальная программа «Цифровая экономика Российской Федерации». Центр компетенций по обеспечению информационной безопасности и противодействию кибератакам в кредитно-финансовой сфере. Надзорная деятельность.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме; - выполнение учебного задания
Конкурентная разведка и	Работа с увольняемыми. Профилактика агентурной деятельности Конкурентная разведка	- работа с учебной, научной и справочной литературой; - конспект;

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
информационное противоборство в кредитно-финансовой сфере.	в США. Конкурентная разведка во Франции. Финансовая разведка в России.	<ul style="list-style-type: none"> - подготовка докладов по теме; - подготовка презентаций по теме; - выполнение учебного задания
Оценка защищенности кредитно-финансовых систем.	Международный стандарт оценки защищенности ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011. Базовые вопросы проверки защищенности. Оценка эффективности и результативности деятельности по управлению ИБ. Измерение, мера измерения, показатель и метрика. Метрики безопасности. Системы анализа защищенности.	<ul style="list-style-type: none"> - работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме; - выполнение учебного задания
Организация системы защиты информации кредитно-финансовых систем	Этапы построения системы защиты информации. Политика безопасности. Оценка эффективности инвестиций в информационную безопасность. Обеспечение компьютерной безопасности учетной информации. Обеспечение информационной безопасности автоматизированных банковских систем (АБС).	<ul style="list-style-type: none"> - работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме; - выполнение учебного задания

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

Форма текущего контроля - контрольная работа.

Примерный перечень вопросов к контрольной работе, примеры заданий контрольных работ

1. Международные стандарты и лучшие практики оценки защищенности банковских систем.
2. Антропогенные уязвимости, риски и угрозы кибербезопасности.
3. Техногенные уязвимости, риски и угрозы кибербезопасности
4. Назначение и виды обрабатываемых данных в автоматизированной системе обработки бэк-офисных банковских операций.

5. Назначение и виды обрабатываемых данных, в автоматизированной системы обработки систем удаленного доступа к счетам физических лиц.
6. Особенности конкурентной разведки в Японии.
7. Конкурентная разведка в Германии.
8. Конкурентная разведка в Швеции.
9. Основные процедуры data mining в задачах финансовой разведки
10. Обнаружение признаков отмывания доходов в транзакциях
11. Обнаружение признаков кибератак
12. Преимущества data mining в конкурентной разведке.
13. Проблемы интерпретации результатов анализа
14. Бенчмаркинг и конкурентная разведка
15. Обеспечение кибербезопасности и киберустойчивости инфраструктуры.
16. Обеспечение информационной безопасности и киберустойчивости прикладного программного обеспечения.
17. Обеспечение информационной безопасности и киберустойчивости технологий обработки данных.
18. Обеспечение информационной безопасности и киберустойчивости финансовых технологий
19. Организация службы информационной безопасности автоматизированных банковских систем.
20. Организация контроля информационной безопасности в кадровых службах.

Примерный перечень вопросов к письменной работе

1. Соотношение антропогенных и техногенных уязвимостей, рисков и угроз кибербезопасности по руководящим нормативным документам Банка России.
2. Техногенные уязвимости, риски и угрозы кибербезопасности, обусловленные несанкционированным доступом к информации в сфере финансов

3. Техногенные уязвимости, риски и угрозы кибербезопасности, обусловленные распространением вредоносных программ в сфере финансов
4. Техногенные уязвимости, риски и угрозы кибербезопасности, обусловленные нарушением правил эксплуатации автоматизированных банковских систем.
5. Антропогенные уязвимости, риски и угрозы кибербезопасности, обусловленные инсайдерами.
6. Антропогенные уязвимости, риски и угрозы кибербезопасности, обусловленные применением методов социальной инженерии
7. Антропогенные уязвимости, риски и угрозы кибербезопасности, обусловленные информационным противоборством в социальных сетях.
8. Ситуация на рынке и действия конкурента в сфере финансов
9. Постановка задач в конкурентной разведке.
10. Профилактическая работа с увольняемыми сотрудниками.
11. Профилактика и противодействие агентурной деятельности

Примерный перечень вопросов для дискуссий

1. Конкурентная разведка в США.
2. Конкурентная разведка во Франции.
3. Финансовая разведка в России.
4. Истоки и принципы бенчмаркинга.
5. Причины отставания России в бенчмаркинге
6. Контент-анализ рекламы и объявлений о приеме на работу.
7. Контент-анализ выступления, интервью или беседы в целях кибербезопасности
8. Процедуры компьютерного анализа текстов в целях кибербезопасности
9. Проблема рекомендаций в отчетах по кибербезопасности

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

Перечень компетенций, формируемых в процессе освоения дисциплины содержится в разделе 2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, владений

компетенция	типовые задания
<p>ПКН-2</p> <p>Способность идентифицировать и измерять финансовые риски, концептуально формировать корпоративную систему управления рисками в условиях развития финтех</p>	<p>Индикатор 1. Владеет современными инструментами и методами анализа и регулирования финансов государственного и негосударственного секторов экономики, деятельности институтов финансово-кредитной сферы</p> <p>Знает принципы обнаружения, идентификации и классификации уязвимостей, рисков и угроз нарушения информационной безопасности объектов кредитно-финансовой сферы</p> <p>Задание 1. Опишите процесс организации проведения обнаружения, идентификации и классификации рисков нарушения информационной безопасности объектов кредитно-финансовой сферы</p> <p>Умеет организовывать обнаружение, идентификацию и классификацию уязвимостей, рисков и угроз нарушения информационной безопасности объектов кредитно-финансовой сферы</p> <p>Задание 1. Составить перечень техногенных уязвимостей и угрозы кибербезопасности, обусловленных несанкционированным доступом к информации в сфере финансов на примере автоматизированной банковской системы</p> <p>Индикатор 2. Демонстрирует способность решения проектно-экономических задач в профессиональной деятельности</p> <p>Знает методы обнаружения, идентификации и классификации уязвимостей, рисков и угроз нарушения информационной безопасности объектов кредитно-финансовой сферы</p> <p>Задание 1. Проанализируйте соотношение антропогенных и техногенных уязвимостей, рисков и угроз кибербезопасности по руководящим нормативным документам Банка России.</p> <p>Умеет проводить обнаружение, идентификацию и</p>

	<p>классификацию уязвимостей, рисков и угроз нарушения информационной безопасности объектов кредитно-финансовой сферы</p> <p>Задание 1. Определить причины отставания России в бенчмаркинге</p> <p>Индикатор 3. Демонстрирует освоение инструментов Финтех</p> <p>Знает методы управления корпоративными рисками</p> <p>Задание 1. Разработайте стратегию управления рисками кибербезопасности на малом предприятии с учетом перспектив развития в Fin Tech России.</p> <p>Умеет выстраивать систему управления корпоративными рисками</p> <p>Задание 1. Определите задачи контент-анализа выступления, интервью или беседы в целях кибербезопасности.</p> <p>Индикатор 4. Владеет методами анализа Big Data, использует для решений профессиональных задач на микро-, мезо- и макроуровнях, в том числе на уровне финансового рынка</p> <p>Знает методы анализа Big Data</p> <p>Задание 1. Опишите основные процедуры data mining в задачах финансовой разведки</p> <p>Умеет использовать методы анализа Big Data для решения профессиональных задач на микро-, мезо- и макроуровнях, в том числе на уровне финансового рынка</p> <p>Задание 1. Проведите классификацию угроз нарушения информационной безопасности типовой информационной системы объектов кредитно-финансовой сферы</p>
--	--

Примерный перечень вопросов к зачету

1. Принципы и методы обнаружения, идентификации и классификации уязвимостей информационной безопасности объектов кредитно-финансовой сферы.
2. Принципы и методы обнаружения, идентификации и классификации рисков нарушения информационной безопасности объектов кредитно-финансовой сферы.
3. Принципы и методы обнаружения, идентификации и классификации угроз нарушения информационной безопасности объектов кредитно-финансовой сферы.
4. Организация проведения обнаружения, идентификации и классификации уязвимостей информационной безопасности объектов кредитно-финансовой сферы.

5. Организация проведения обнаружения, идентификации и классификации рисков нарушения информационной безопасности объектов кредитно-финансовой сферы

6. Организация проведения обнаружения, идентификации и классификации угроз нарушения информационной безопасности объектов кредитно-финансовой сферы

7. Практика организации и обеспечения обнаружения, идентификации и классификации уязвимостей информационной безопасности объектов кредитно-финансовой сферы.

8. Практика организации и обеспечения обнаружения. Идентификации и классификации рисков нарушения информационной безопасности объектов кредитно-финансовой сферы.

9. Практика организации и обеспечения обнаружения. Идентификации и классификации угроз нарушения информационной безопасности объектов кредитно-финансовой сферы.

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

Нормативные акты

1. Федеральный закон «О национальной платежной системе» от 27.06.2011 N 161-ФЗ

2. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ

3. Указание Банка России N 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств»

4. Положение Банка России N 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств»

5. Письмо Банка России от 17 ноября 2011 г. № 015-16-9/4713 «О средствах защиты информации, применяемых при обработке персональных данных»

6. Указание Банка России от 5 июня 2013 г. N 3007-У «О внесении изменений в положение Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении

переводов денежных средств»

7. Письмо от 5 августа 2013 г. N 146-Т «О рекомендациях по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием интернет»

8. Письмо Банка России от 07.12.2007 N 197-Т «О рисках при дистанционном банковском обслуживании».

9. Письмо Банка России от 31 марта 2008 г. N 36-Т «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга»

10. Письмо Банка России от 02.10.2009 N 120-Т О памятке «О мерах безопасного использования банковских карт».

11. Письмо Банка России от 22 ноября 2010 г. N 154-Т «О рекомендациях по раскрытию информации об основных условиях использования банковской карты и о порядке урегулирования конфликтных ситуаций, связанных с ее использованием».

12. Письмо Банка России от 24 марта 2014 г. N 49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности».

Рекомендуемая литература:

а) основная:

13. Бекетнова, Ю.М. Международные основы и стандарты информационной безопасности финансово-экономических систем: учебное пособие/ Ю.М. Бекетнова, Г.О.Крылов, С.Л. Ларионова; Финансовый университет при Правительстве Российской Федерации. - Москва: Прометей, 2018. - 171 с. – Текст: непосредственный. – То же. – ЭБС Университетская библиотека online. – URL: http://biblioclub.ru/index.php?page=book_red&id=494850&sr=1 (дата обращения: 07.10.2019). – Текст: электронный.

14. Бачило И.Л. Актуальные проблемы информационного права: учебник /под ред. И.Л.Бачило, М.А. Лапиной. - Москва: Юстиция, 2016. - 534 с. – То же. – 2019. – ЭБС Book.ru. – URL: <https://www.book.ru/book/931052> (дата обращения: 07.10.2019). – Текст: электронный.

б) дополнительная:

15. Бекетнова, Ю.М. Модели и методы решения аналитических задач финансового мониторинга: монография / Ю.М.Бекетнова, Г.О.Крылов, С.Л.Ларионова; Финансовый университет при Правительстве Российской Федерации. - Москва: Прометей, 2018. - 274 с. – Текст: непосредственный. – То же. - ЭБС Университетская библиотека online. – URL: http://biblioclub.ru/index.php?page=book_red&id=494851&sr=1 (дата обращения: 07.10.2019). – Текст: электронный.

16. Крылов, Г.О. Базовые понятия информационной безопасности: учебное пособие / Г.О.Крылов, С.Л.Ларионова, В.Л. Никитина. — Москва: Русайнс, 2020. — 257 с. — URL: <https://book.ru/book/932492> (дата обращения: 07.10.2019). — Текст: электронный.

17. Воронцова, С.В. Обеспечение информационной безопасности в банковской сфере (Законность и правопорядок): монография / С.В. Воронцова. – Москва: КноРус, 2017. – 160 с. – ЭБС Book.ru. – URL: <https://www.book.ru/book/921936> (дата обращения: 07.10.2019). - Текст: электронный.

18. Вдовин, В.М. Информационные технологии в финансово-банковской сфере / В.М. Вдовин, Л.Е. Суркова. – Москва: Дашков и К, 2018. – 304 с. – ЭБС Znanium.com. - URL: <http://znanium.com/catalog/product/450752> (дата обращения 07.10.2019). - 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 библиотека Финансового университета (ЭБ) <http://elib.fa.ru/> (<http://library.fa.ru/files/elibfa.pdf>)
5. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
6. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>

7. Электронно-библиотечная система Znaniум <http://www.znanium.com>

8. «Деловая онлайн библиотека» издательства «Альпина Паблишер»
<http://lib.alpinadigital.ru/en/library>

9. Электронно-библиотечная система издательства «ЮРАЙТ»
<https://www.biblio-online.ru/>

10. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>

10. Методические указания для обучающихся по освоению дисциплины

Студентам при подготовке следует использовать нормативные документы Финансового университета, а именно, - Приказ Финуниверситета от 11.05.2021 № 1040/о «Об утверждении методических рекомендаций по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры в Финансовом университете» (см. сайт Финансового Университета: на главной странице раздел «Наш университет»; далее «Единая правовая база Финуниверситета»; подраздел «Организация учебного процесса» - Нормативные документы по самостоятельной работе), использовать методические рекомендации преподавателей департамента.

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

1. Windows, Microsoft Office
2. Антивирус ESET Endpoint Security

11.2 Современные профессиональные базы данных и информационные справочные системы

1. Информационно-правовая система «Гарант»
2. Информационно-правовая система «Консультант Плюс»
3. Электронная энциклопедия: <http://ru.wikipedia.org/wiki/Wiki>
4. Система комплексного раскрытия информации «СКРИН» -
<http://www.skrin.ru/>

11.3 Сертифицированные программные и аппаратные средства защиты информации

Не предусмотрены.

12. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.

Занятия по дисциплине проводятся в аудиториях, оборудованных мультимедийными комплексами, компьютерами с выходом в Интернет.