

**Федеральное государственное автономное образовательное  
учреждение высшего образования  
«Московский физико-технический институт  
(национальный исследовательский университет)»**

**УТВЕРЖДЕНО**

**Директор по цифровизации  
образования**

**Д.И. Гриц**

	<b>Рабочая программа дисциплины (модуля)</b>
<b>по дисциплине:</b>	Кибербезопасность финансовых услуг
<b>по направлению:</b>	Бизнес-информатика
<b>профиль подготовки:</b>	Финансовые технологии и аналитика центр дополнительного, дополнительного профессионального и онлайн-образования "Пуск" центр дополнительного, дополнительного профессионального и онлайн-образования "Пуск"
<b>курс:</b>	2
<b>квалификация:</b>	магистр

Семестр, формы промежуточной аттестации: 4 (весенний) - Экзамен

Аудиторных часов: 30 всего, в том числе:

лекции: 12 час.

семинары: 18 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 75 час.

Подготовка к экзамену: 30 час.

Всего часов: 135, всего зач. ед.: 3

Программу составили:

Е.А. Савицкая, начальник отдела

О.А. Культепина, методист

Программа обсуждена на заседании центра дополнительного, дополнительного профессионального и  
онлайн-образования "Пуск" 13.06.2022

## Аннотация

В рамках дисциплины “Кибербезопасность финансовых услуг” обучающиеся осваивают компетенции по применению комплекса мероприятий в системе защиты информации на основе реализации требований к информационной безопасности в финансовой сфере.

### 1. Цели и задачи

#### Цель дисциплины

- формирование у обучающихся системно-целостного видения проблем обеспечения кибербезопасности, представления о природе возникновения типичных угроз, а также навыков практической реализации мероприятий защиты от кибератак в контуре информационных систем финансовой сферы.

#### Задачи дисциплины

- изучение основных положений, понятий и категорий теоретических основ функционирования систем информационной безопасности финансовых систем;
- изучение основ и принципов организации современных проблем организационного обеспечения информационной безопасности;
- изучение организации работы и порядка применения терминологии организационного обеспечения информационной безопасности;
- изучение основных направлений и методов организационной защиты информации в финансовых системах, формирование умений в разработке проектов функционирования систем организационной защиты информации финансовых систем;
- развитие умения применять методологию обеспечения кибербезопасности информационных систем и информационных ресурсов, используемых в профессиональной деятельности;
- формирование навыков работы в организации процессов управления системами организационной защиты информации финансовых систем.

### 2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-3 Способен принимать решения, осуществлять стратегическое планирование и прогнозирование в профессиональной деятельности с использованием современных методов и программного инструментария сбора, обработки и анализа данных, интеллектуального оборудования и систем искусственного интеллекта	ОПК-3.1 Владеет методами стратегического планирования и прогнозирования в профессиональной деятельности
	ОПК-3.2 Самостоятельно выбирает и обосновывает выбор современных методов и программного инструментария сбора, обработки и анализа данных
	ОПК-3.3 Владеет аналитическими и вычислительными методами решения, задач, понимает и учитывает на практике границы применимости получаемых решений
ПК-16 Способен готовить аналитические материалы для оценки мероприятий и выработки стратегических решений в области ИКТ	ПК-16.1 Эффективно применяет в ходе профессиональной деятельности методы и инструментари анализ данных
	ПК-16.2 Знает методы подготовки аналитических материалов для оценки мероприятий и выработки стратегических решений в области ИКТ

### 3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- методы защиты информации в финансовых системах;
- основы защиты персональных данных в финансовых системах;
- организационные основы деятельности подразделений защиты информации в финансовых системах;
- методику оценки угроз безопасности информации;
- методы фишинга в кредитно-финансовой сфере;
- психология фишинга.

уметь:

- организовывать работу с персоналом по вопросам защиты информации в банковской сфере, в том числе в рамках SOC;
- проводить анализ событий информационной безопасности;
- обеспечивать безопасность интернет-платежей;
- использовать в профессиональной деятельности матрицу MITRE ATT&CK.

владеть:

- навыками определения источников и способов реализации (возникновения) угроз информационной безопасности;
- восстановление систем(файлов) после атаки шифровальщика;
- навыками использования DLP-систем, систем IDS/IPS.

#### 4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

##### 4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Введение в кибербезопасность финансовых услуг	2	4		15
2	Специфика технологии защищенного документооборота	4	2		20
3	Принципы построения системы кибербезопасности. Определение уязвимостей финансовых систем и выбор средств защиты. Формирование требований к построению систем криптографической и стеганографической защиты.	4	6		20
4	Киберпреступность и способы её предотвращения	2	6		20
Итого часов		12	18		75
Подготовка к экзамену		30 час.			
Общая трудоёмкость		135 час., 3 зач.ед.			

##### 4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 4 (Весенний)

###### 1. Введение в кибербезопасность финансовых услуг

Задачи кибербезопасности в финансовых системах. Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз. Основы файловой системы. Требования к системам защиты информации.

###### 2. Специфика технологии защищенного документооборота

Антивирусы и защита электронного документооборота от несанкционированного доступа. Общая характеристика сетей и протоколов передачи данных. Методологические рекомендации по анализу режимов работы кибернетических систем.

3. Принципы построения системы кибербезопасности. Определение уязвимостей финансовых систем и выбор средств защиты. Формирование требований к построению систем криптографической и стеганографической защиты.

Общие требования к паролям. Симметричное и асимметричное шифрование. Хэш-функция и электронная подпись и протоколы электронных данных. Защищенные каналы данных облачные технологии и защищённый документооборот.

4. Киберпреступность и способы её предотвращения

Нормативно-правовые акты и стандарты по кибербезопасности. Преступления в сфере информационных технологий.

## **5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)**

Занятия по учебной дисциплине проводятся с использованием дистанционных образовательных технологий. Каждый обучающийся обеспечен доступом к образовательной платформе <https://netology.ru/>.

## **6.Перечень рекомендуемой литературы**

### Основная литература

1. Введение в информационную безопасность автоматизированных систем, Электронная версия печатной публикации / В. В. Бондарев. — Москва, МГТУ им. Н.Э. Баумана, 2018
2. Информационная безопасность и защита информации / Е. К. Баранова, А. В. Бабаш, Москва, РИОР : ИНФРА-М, 2020

### Дополнительная литература

- 1.
2. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс], Электрон. версия печ. публикации / В. Ф. Шаньгин. — М., ДМК Пресс, 2010

Рекомендуемая литература для самостоятельного изучения:

1. Федеральный закон 63-ФЗ «Об электронной цифровой подписи»
2. Федеральный закон 98-ФЗ «О Коммерческой тайне»
3. Федеральный закон 149-ФЗ «Об информации, информационных технологиях и о защите информации»
4. Федеральный закон 152-ФЗ «О персональных данных»
5. Постановление правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
6. Федеральный закон 187-ФЗ «Критическая информационная инфраструктура»
7. Стандарт Банка России СТО БР ИББС-1.0-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" (принят и введен в действие распоряжением Банка России от 17 мая 2014 г. N Р-399)
8. Письмо Банка России от №49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности»
9. Положение Банка России № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств»
10. Положение Банка России №552-П "О требованиях к защите информации в платежной системе Банка России
11. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер».

## **7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)**

1. Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/132242> (дата обращения: 03.06.2022). — Режим доступа: для авториз. пользователей.
2. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко. — Ставрополь : СКФУ, 2015. — 222 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/155247> (дата обращения: 03.06.2022). — Режим доступа: для авториз. пользователей.
3. Рагозин, Ю. Н. Организация и управление подразделением защиты информации на предприятии : учебное пособие / Ю. Н. Рагозин, В. А. Мельник. — Санкт-Петербург : Интермедия, 2019. — 240 с. — ISBN 978-5-4383-0180-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/161357> (дата обращения: 03.06.2022). — Режим доступа: для авториз. пользователей.
4. Steganography Online ; <http://stylesuxx.github.io/steganography/>
5. Online encrypt tool ; [https://www.tools4noobs.com/online\\_tools/encrypt/](https://www.tools4noobs.com/online_tools/encrypt/)
6. Image Steganography ; <https://incoherency.co.uk/image-steganography/>
7. Crypt-Online ; <http://crypt-online.narod.ru>

## **8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)**

1. Образовательная платформа <https://netology.ru/>
2. Webinar.ru
3. Zoom
4. Google Drive

## **9. Методические указания для обучающихся по освоению дисциплины (модуля)**

Студент, изучающий дисциплину, должен с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике. В результате изучения дисциплины студент должен знать основные определения дисциплины, уметь применять полученные знания для решения различных задач.

Успешное освоение курса требует:

- посещения всех занятий, предусмотренных учебным планом по дисциплине;
- ведения конспекта занятий;
- напряжённой самостоятельной работы студента.

Самостоятельная работа включает в себя:

- чтение рекомендованной литературы;
- проработку учебного материала, подготовку ответов на вопросы, предназначенных для самостоятельного изучения;
- решение задач, предлагаемых студентам на занятиях;
- подготовку к выполнению заданий текущей и промежуточной аттестации.

Показателем владения материалом служит умение без конспекта отвечать на вопросы по темам дисциплины.

Важно добиться понимания изучаемого материала, а не механического его запоминания. При затруднении изучения отдельных тем, вопросов, следует обращаться за консультациями к преподавателю.

Возможен промежуточный контроль знаний студентов в виде решения задач в соответствии с тематикой занятий.

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

<b>по направлению:</b>	Бизнес-информатика		
<b>профиль подготовки:</b>	Финансовые технологии и аналитика	▲	▲
	онлайн-образования "Пуск"	▲	▲
	онлайн-образования "Пуск"		
<b>курс:</b>	2		
<b>квалификация:</b>	магистр		

Семестр, формы промежуточной аттестации: 4 (весенний) - Экзамен

**Разработчики:**

Е.А. Савицкая, начальник отдела

О.А. Культепина, методист

## 1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-3 Способен принимать решения, осуществлять стратегическое планирование и прогнозирование в профессиональной деятельности с использованием современных методов и программного инструментария сбора, обработки и анализа данных, интеллектуального оборудования и систем искусственного интеллекта	ОПК-3.1 Владеет методами стратегического планирования и прогнозирования в профессиональной деятельности
	ОПК-3.2 Самостоятельно выбирает и обосновывает выбор современных методов и программного инструментария сбора, обработки и анализа данных
	ОПК-3.3 Владеет аналитическими и вычислительными методами решения, задач, понимает и учитывает на практике границы применимости получаемых решений
ПК-16 Способен готовить аналитические материалы для оценки мероприятий и выработки стратегических решений в области ИКТ	ПК-16.1 Эффективно применяет в ходе профессиональной деятельности методы и инструментари анализа данных
	ПК-16.2 Знает методы подготовки аналитических материалов для оценки мероприятий и выработки стратегических решений в области ИКТ

## 2. Показатели оценивания компетенций

В результате изучения дисциплины «Кибербезопасность финансовых услуг» обучающийся должен:

### знать:

- методы защиты информации в финансовых системах;
- основы защиты персональных данных в финансовых системах;
- организационные основы деятельности подразделений защиты информации в финансовых системах;
- методику оценки угроз безопасности информации;
- методы фишинга в кредитно-финансовой сфере;
- психология фишинга.

### уметь:

- организовывать работу с персоналом по вопросам защиты информации в банковской сфере, в том числе в рамках SOC;
- проводить анализ событий информационной безопасности;
- обеспечивать безопасность интернет-платежей;
- использовать в профессиональной деятельности матрицу MITRE ATT&CK.

### владеть:

- навыками определения источников и способов реализации (возникновения) угроз информационной безопасности;
- восстановление систем(файлов) после атаки шифровальщика;
- навыками использования DLP-систем, систем IDS/IPS.

## 3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

Во время текущего контроля студент должен уметь ответить на следующие вопросы:

1. Необходимость обеспечения безопасности в информационных системах.
2. Нормативно-правовые аспекты информационной безопасности.
3. Классификация угроз безопасности информационных объектов.
4. Основные виды каналов утечки информации.
5. Умышленные и неумышленные угрозы информационной безопасности.
6. Внешние угрозы информационной безопасности.
7. Мотивы и цели компьютерных преступлений.
8. Объекты информационной безопасности в финансовых учреждениях.
9. Программно - технические методы обеспечения информационной безопасности.

10. Идентификация и аутентификация.
11. Государственное регулирование информационной безопасности в России.
12. Несанкционированный доступ и защита от него.
13. Типы компьютерных вирусов и защита от них.
14. Человеческие факторы, обуславливающие информационные угрозы.
15. Субъективная сторона компьютерных преступлений. Объективная сторона компьютерных преступлений.
16. Способы совершения компьютерных преступлений.
17. Причины и условия, способствующие совершению компьютерных преступлений.
18. Экономическая информация как объект безопасности.
19. Перечень сведений, которые не могут составлять коммерческую тайну.
20. Причины разглашения конфиденциальной информации.
21. Разглашение и утечка информации.
22. Стратегия злоумышленника при несанкционированном доступе.
23. Организация конфиденциального делопроизводства.
24. Структура службы безопасности компании.
25. Основные понятия информационной безопасности экономических систем.
26. Понятия информационных угроз и их виды.
27. Вредоносные программы.
28. Подходы, принципы, методы и средства обеспечения безопасности.
29. Организационно-техническое обеспечение компьютерной безопасности.
30. Электронная цифровая подпись и особенности ее применения.
31. Организация системы защиты информации экономических систем.
32. Этапы построения системы защиты информации.
33. Политика безопасности.
34. Оценка эффективности инвестиций в информационную безопасность.
35. Обеспечение информационной безопасности автоматизированных банковских систем (АБС).
36. Информационная безопасность электронной коммерции (ЭК).
37. Обеспечение компьютерной безопасности учетной информации.
38. Сущность криптографических методов.
39. Типы и субъекты информационных угроз.
40. Общая методология организационного обеспечения ИБ на уровне крупных поставщиков информационных систем.
41. Инфраструктура публичных ключей.
42. Страхование информационных рисков.
43. Стандарт ISO/IEC 27005:2011 – «Информационная технология. Методы и средства обеспечения безопасности. Управление рисками ИБ.»
44. Стандарт ГОСТ Р ИСО/МЭК 27005:2010 – «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска ИБ.»
45. Стандарт 7799-3:2006 – руководство по управлению рисками ИБ.
46. Что такое риск ИБ. Пример рисков ИБ для ОС.
47. Взаимосвязь основных понятий ИБ в системе управления рисками.
48. Риск нарушения ИБ.
49. Управление рисками и риск - менеджмент ИБ.
50. Основные элементы управления рисками ИБ применительно к понятиям ИБ.
51. Задачи управления рисками ИБ.
52. Составляющие процесса управления рисками ИБ.
53. Анализ и идентификация рисков.
54. Оценка и обработка рисков ИБ.
55. Основные задачи менеджмента в сфере ИБ.
56. Что подразумевается под комплектностью решений задач ИБ?
57. Что включает в себя управление человеческими ресурсами в рамках управления ИБ?
58. Что подразумевает безопасность информационной инфраструктуры?



#### 4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

Примеры вопросов:

1. Задачи кибербезопасности в финансовых системах.
2. Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз.
3. Основы файловой системы.
4. Требования к системам защиты информации.
5. Антивирусы и защита электронного документооборота от несанкционированного доступа.
6. Общая характеристика сетей и протоколов передачи данных.
7. Методологические рекомендации по анализу режимов работы кибернетических систем.
8. Общие требования к паролям.
9. Симметричное и асимметричное шифрование.
10. Хэш-функция и электронная подпись и протоколы электронных данных.
11. Защищенные каналы данных облачные технологии и защищённый документооборот.
12. Нормативно-правовые акты и стандарты по кибербезопасности.
13. Преступления в сфере информационных технологий.

Билет 1.

Прокомментируйте алгоритм действий и требование к системам при выполнении задач:

- распознавание и обнаружение инцидентов кибербезопасности;
- проведение простых расследований;
- подготовка и реализация эффективного плана реагирования на инциденты.

Билет 2

Прокомментируйте алгоритм действий и требование к системам при выполнении задач:

- проведение криминалистических расследований в системах;
- создание эффективного плана расследования инцидентов в системах;
- сбор физических и цифровых улик и их анализ.

#### Критерии оценивания

Оценка отлично (10 баллов) - выставляется обучающемуся, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины, проявляющему интерес к данной предметной области, продемонстрировавшему умение уверенно и творчески применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично (9 баллов) - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично (8 баллов) - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, правильное обоснование принятых решений, с некоторыми недочетами.

Оценка хорошо (7 баллов) - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но недостаточно грамотно обосновывает полученные результаты.

Оценка хорошо (6 баллов) - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности.

Оценка хорошо (5 баллов) - выставляется студенту, если он в основном знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач достаточно большое количество неточностей.

Оценка удовлетворительно (4 балла) - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он освоил основные разделы учебной программы, необходимые для дальнейшего обучения, и может применять полученные знания по образцу в стандартной ситуации.

Оценка удовлетворительно (3 балла) - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, допускающему ошибки в формулировках базовых понятий, нарушения логической последовательности в изложении программного материала, слабо владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и с трудом применяет полученные знания даже в стандартной ситуации.

Оценка неудовлетворительно (2 балла) - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных принципов и не умеет использовать полученные знания при решении типовых задач.

Оценка неудовлетворительно (1 балл) - выставляется студенту, который не знает основного содержания учебной программы дисциплины, допускает грубейшие ошибки в формулировках базовых понятий дисциплины и вообще не имеет навыков решения типовых практических задач.

## **5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности**

Экзамен по дисциплине проводится в форме выполнения итогового задания.