Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ФИНАНСОВЫХ ТЕХНОЛОГИЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

КАФЕДРА ФИНАНСОВОГО МОНИТОРИНГА

ОДОБРЕНО УМС ИФТЭБ

Протокол № 545-6

от 28.08.2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки (специальность) — [1] 10.05.04 Информационно-аналитические системы безопасности

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	В форме практической подготовки, час.	СРС, час.	КСР, час.	Форма(ы) контроля, экз./зач./КР/КП
3	2	72	32	0	0		40	0	З
Итого	2	72	32	0	0	0	40	0	

АННОТАЦИЯ

Дисциплина посвящена организационному и правовому обеспечению информационной безопасности: рассматриваются международные, российские и отраслевые документы по защите информации, практика их правоприменения, а также организация защиты информации на уровне государства и предприятия. Изучаются правовая защита сведений ограниченного доступа и сферы компьютерной информации, порядок проектирования системы защиты информации и разбор современных кибер-инцидентов. На практических занятиях студенты работают с организационно-правовыми документами, решают задачи на основе реальных информационных систем.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью преподавания дисциплины является ознакомление студентов с основными понятиями в области организационно-правового обеспечения безопасности процессов информатизации и защиты информационной сферы.

Задачи дисциплины:

- раскрытие предмета и базовых понятий организационно-правового обеспечения информационной безопасности;
- изучение основных законов, связанных с организационно-правовым обеспечением информационной безопасности, их содержания и взаимосвязи;
- изучение основных способов правового обеспечения безопасности в информационной сфере.

Таким образом, дисциплина является неотъемлемой составной частью профессиональной подготовки студентов. Изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как строгость в суждениях, творческое мышление, организованность и работоспособность, дисциплинированность, самостоятельность и ответственность.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Для успешного освоения дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

- Информатика;
- Информационная безопасность;
- Программирование (алгоритмы и структуры данных);
- Языки программирования;
- Право.

Знания, полученные при изучении дисциплины, используются при освоении дисциплин:

- Безопасность электронного документооборота;
- Безопасность информационных и аналитических систем;
- Кибербезопасность автоматизированных систем;
- Информационное право;
- Экономическая безопасность;

при прохождении учебной практики и производственной практики (НИР), а также для подготовки выпускной квалификационной работы (ВКР).

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**
ОПК-5 [1] – Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	З-ОПК-5 [1] – знать нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации У-ОПК-5 [1] – уметь применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации В-ОПК-5 [1] – владеть нормативными правовыми актами, нормативными и методическими документами, регламентирующими деятельность по защите информации
ОПК-6 [1] – Способен при решении профессиональных задач проверять выполнение требований защиты информации ограниченного доступа в информационно-аналитических системах в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	З-ОПК-6 [1] – знать нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю необходимые при решении задач профессиональной деятельности У-ОПК-6 [1] – уметь организовать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при решении задач профессиональной деятельности В-ОПК-6 [1] – владеть принципами организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при решении задач профессиональной деятельности

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	**Задачи воспитания (код)**
Профессиональное воспитание	Создание условий, обеспечивающих, формирование культуры финансовой безопасности (В44)
Профессиональное воспитание	Создание условий, обеспечивающих,

	формирование ориентации на неукоснительное соблюдение нравственных и правовых норм в профессиональной деятельности (В45)

5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	3 Семестр						
1	Первый раздел	1-8	16/0/0		25	КИ-8	З-ОПК-5, У-ОПК-5, В-ОПК-5, З-ОПК-6, У-ОПК-6, В-ОПК-6
2	Второй раздел	9-16	16/0/0		25	КИ-16	З-ОПК-5, У-ОПК-5, В-ОПК-5, З-ОПК-6, У-ОПК-6, В-ОПК-6
	Итого за 3 Семестр		32/0/0		50		
	Контрольные мероприятия за 3 Семестр				50	З	З-ОПК-5, У-ОПК-5, В-ОПК-5, З-ОПК-6, У-ОПК-6, В-ОПК-6

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	Полное наименование
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	3 Семестр	32	0	0
1-8	**Первый раздел**	16	0	0
1 - 2	**Концептуальные основы информационной безопасности** История возникновения органов защиты информации. ФСБ. ФСТЭК. Понятие "информационная безопасность". Интересы государства, личности, общества и их защита. Носители информации. Основные виды организационных средств обеспечения информационной безопасности.	Всего аудиторных часов 4 Онлайн 0	0 0	0 0
3 - 6	**Основные принципы и условия организационной защиты информации.** Основные нормативные документы, регламентирующие организацию защиты информации на уровне государства и предприятия. Основные подходы и требования к организации системы защиты информации. Основные силы и средства, используемые для организации защиты информации. Грифы секретности. Порядок отнесения сведений к конфиденциальной, секретной коммерческой информации. Основания и порядок рассекречивания сведений и их носителей. Организация допуска и доступа персонала к защищаемой информации. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации. Организация внутриобъектового и пропускного режимов на предприятии.Организация охраны предприятий. Организация защиты информации при проведении совещаний, в ходе издательской и рекламной деятельности	Всего аудиторных часов 8 Онлайн 0	0 0	0 0
7 - 8	**Организация аналитической работы и контроля состояния защиты конфиденциальной информации.** Организация аналитической работы и контроля состояния защиты конфиденциальной информации. Организация ТЗИ. Организация защиты в АС. Организация защиты информации в рамках 187-ФЗ.	Всего аудиторных часов 4 Онлайн 0	0 0	0 0
9-16	**Второй раздел**	16	0	0
9 - 12	**Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну.** Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну. Уголовно-правовая защита сведений, составляющих гос. тайну. Уголовно-правовая защита в сфере компьютерной информации. Статья УК РФ по безопасности объектов КИИ. Защита интеллектуальной собственности. Защита бренда в Интернете.	Всего аудиторных часов 8 Онлайн 0	0 0	0 0
13 - 16	**Известные хакерские инциденты.** Известные хакерские инциденты.	Всего аудиторных часов 8	0	0

	Истории расследования современных компьютерных инцидентов. Организация и проведение служебного расследования. Практика проведения расследования по различным статьям УК РФ.	Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Дисциплина сформирована как курс лекций, при чтении которых используются современные мультимедийные средства. Для самостоятельной работы студентов используются специально подготовленный конспект лекций и другая рекомендуемая преподавателем учебная литература.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ОПК-5	З-ОПК-5	З, КИ-8, КИ-16
	У-ОПК-5	З, КИ-8, КИ-16
	В-ОПК-5	З, КИ-8, КИ-16
ОПК-6	З-ОПК-6	З, КИ-8, КИ-16
	У-ОПК-6	З, КИ-8, КИ-16
	В-ОПК-6	З, КИ-8, КИ-16

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-х балльной шкале</th><th>Отметка о зачете</th><th>Оценка ECTS</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td rowspan="7">«зачтено»</td><td>A</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>ниже 60</td><td>2 – «неудовлетворительно»</td><td>«не зачтено»</td><td>F</td></tr>
</table>

Оценка «отлично» соответствует глубокому и прочному освоению материала программы обучающимся, который последовательно, четко и логически стройно излагает свои ответы, умеет тесно увязывать теорию с практикой, использует в ответах материалы монографической литературы.

Оценка «хорошо» соответствует твердым знаниям материала обучающимся, который грамотно и, по существу, излагает свои ответы, не допуская существенных неточностей.

Оценка «удовлетворительно» соответствует базовому уровню освоения материала обучающимся, при котором освоен основной материал, но не усвоены его детали, в ответах присутствуют неточности, недостаточно правильные формулировки, нарушения логической последовательности.

Отметка «зачтено» соответствует, как минимум, базовому уровню освоения материала программы, при котором обучающийся владеет необходимыми знаниями, умениями и навыками, умеет применять теоретические положения для решения типовых практических задач.

Оценку «неудовлетворительно» / отметку «не зачтено» получает обучающийся, который не знает значительной части материала программы, допускает в ответах существенные ошибки, не выполнил все обязательные задания, предусмотренные программой. Как правило, такие обучающиеся не могут продолжить обучение без дополнительных занятий.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ В 60 Защита информации : учебное пособие для вузов, Внуков А. А., Москва: Юрайт, 2024

2. ЭИ С 89 Информационная безопасность : учебное пособие для вузов, Суворова Г. М., Москва: Юрайт, 2024

3. ЭИ П 54 Организационное и правовое обеспечение информационной безопасности : учебник для вузов, Полякова Т. А., Ниесов В. А., Чубукова С. Г., Москва: Юрайт, 2024

4. ЭИ П 54 Организационное и правовое обеспечение информационной безопасности : учебник для вузов, Полякова Т. А., Ниесов В. А., Чубукова С. Г., Москва: Юрайт, 2025

5. ЭИ Ш 13 Правовое регулирование информационных отношений в сфере обработки персональных данных : учебное пособие для вузов, Федотов М. А., Шаблинский И. Г., Москва: Юрайт, 2024

6. ЭИ Ж70 Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах : монография, Завьялова Д.В., Жижина М.В., Москва: Проспект, 2023

7. ЭИ З-93 Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов, Вехов В. Б. [и др.], Москва: Юрайт, 2024

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 М 21 Глобальная культура кибербезопасности : , Малюк А.А., Москва: Горячая линия - Телеком, 2018

2. 004 М 21 Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. : учеб. пособие для вузов., Малюк А.А., Москва: Горячая линия -Телеком, 2018

3. 34 С28 Правовая защита информации в коммерческих организациях : учебное пособие для вузов, Северин В.А., Москва: Академия, 2009

4. ЭИ К 61 Расследование преступлений с использованием компьютерной информации из сети Интернет : , Васюков В.Ф., Колычева А.Н. , Москва: Проспект, 2020

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. Библиотека ГОСТов и стандартов (http://www.standartov.ru)

2. Правовой портал "Консультант Плюс" (www.consultant.ru)

3. Информационно-правовая система "Гарант" (www. garant.ru)

4. Информационно-правовая система "Кодекс" (www.kodeks.ru)

5. ИНТУИТ Национальный открытый университет (https://intuit.ru/)

6. ИС "Единое окно доступа к образовательным ресурсам" (http://window.edu.ru/)

7. Официальный интернет-портал правовой информации (http://pravo.gov.ru/)

8. ITSec.Ru. Медиаплатформа, посвящённая информационной безопасности (itsec.ru.)

https://online.mephi.ru/

http://library.mephi.ru/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Изучение дисциплины следует начинать с проработки учебной программы, уделяя особое внимание целям и задачам, структуре и содержанию курса, и заранее спланировать учебное время в соответствии с планом лекций и графиком контроля знаний. Во время лекций рекомендуется вести конспект, кратко и логично фиксируя основные положения и выводы, а сразу после занятия просмотреть его и отметить материал, вызывающий затруднения. Для самостоятельной работы следует опираться на основную литературу из списка рабочей программы - учебные пособия по защите информации, информационной безопасности и ее организационно-правовому обеспечению, а также работы по правовому регулированию обработки персональных данных и расследованию преступлений в сфере компьютерной информации. Дополнительная литература (в том числе труды по политике безопасности критических информационных систем и правовой защите информации в коммерческих организациях) поможет углубить отдельные темы и подготовиться к разбору практических задач. Доступ к изданиям обеспечивается через библиотеку и электронные ресурсы университета (online.mephi.ru, library.mephi.ru), поэтому перед консультацией полезно заранее найти рекомендуемые главы и ознакомиться с ними. Если самостоятельно разобраться в вопросе не удалось, стоит сформулировать его и обратиться к преподавателю на консультации или ближайшей лекции; для успешного освоения дисциплины необходимы регулярное посещение лекций, выполнение всех домашних заданий и постоянный самоконтроль по контрольным вопросам.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Учебный курс строится на интегративной основе и сочетает теоретические знания, получаемые на лекциях, с практическими навыками разбора организационно-правовых документов и решения задач, основанных на реальных информационных системах. Содержание дисциплины распределяется между лекционной и практической частями по принципу дополняемости: практические занятия не дублируют лекции, а посвящены рассмотрению практических примеров и конкретизации материала, введенного на лекции, при этом в лекционном курсе главное место отводится общетеоретическим проблемам. Преподавателю следует оптимизировать учебный процесс в плане отбора материала и методики его организации, а также контроля текущей учебной работы, повышая статус внеаудиторной самостоятельной работы как полноценного и обязательного вида учебно-познавательной деятельности студентов. Со стороны преподавателя должен быть установлен контакт со студентами, которые должны быть информированы о порядке прохождения курса, его особенностях и учебно-методическом обеспечении. Преподаватель дает методические

рекомендации по самостоятельному изучению проблем, характеризуя пути и средства достижения поставленных задач, а также высказывает советы по изучению учебной литературы, самостоятельной работе и работе на занятиях. При рассмотрении разделов о правовой защите сведений и расследовании компьютерных инцидентов целесообразно опираться на действующие нормативные акты и практику правоприменения, ориентируя студентов на строгость суждений и самостоятельность.

Автор(ы):

Рычков Вадим Александрович