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

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КРИПТОЛОГИИ И ДИСКРЕТНОЙ МАТЕМАТИКИ

ОДОБРЕНО УМС ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки (специальность) [1] 10.03.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
5	2	72	32	0	0		8-40	0	З
Итого	2	72	32	0	0	0	8-40	0	

Москва, 2020

АННОТАЦИЯ

Нормативно-правовые документы являются одной из важных составляющих информационной безопасности. Каждый специалист должен знать, понимать и уметь применять законодательные акты в области информационной безопасности.

На лекционных занятиях рассматриваются международные, российские и отраслевые документы по защите информации и практика их правоприменения. Изучается УК РФ в части статей по информационной безопасности и защите информации. Изучается организация защиты информации на уровне государства (с учетом 187-ФЗ) и предприятия, необходимые ресурсы (технические и программные, сотрудники), процесс проектирования системы защиты информации на предприятии, рассматриваются совершенные и современные кибер-инциденты.

В ходе практических занятий со студентами разбираются важнейшие организационно-правовые документы, объясняется в чем их смысл и как применить данный документ в реальной жизни. Студенты решают задачи, которые разработаны специально для курса и основаны на реальных информационных системах. По итогам курса студенты самостоятельно делают проект, в котором применяют полученные знания

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью преподавания дисциплины «Организационно-правовое обеспечение информационной безопасности» 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 «Организационно-правовое обеспечение информацион-ной безопасности» является неотъемлемой составной частью профессиональной подго-товки по 10.03.01 «Информационная безопасность». 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

Дисциплина «Организационно-правовое обеспечение информационной безопасности» относится к базовым дисциплинам общепрофессионального модуля. Данная дисциплина является необходимым элементом, обеспечивающим формирование культуры информационной безопасности как необходимого качества любого специалиста, осуществляющего профессиональную деятельность в условиях развития информационного общества. Для

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

- «Философия»;
- «Основы управленческой деятельности»,
- «Документоведение»,
- «Основы информационной безопасности».

Знания, полученные при изучении дисциплины «Организационно-правовое обеспечение информационной безопасности», используются при изучении дисциплин:

- «Метрология, стандартизация и сертификация»,
- «Управление информационной безопасности».

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-10 [1] – Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	З-ОПК-10 [1] – знать способы создания политики информационной безопасности организации и комплекс мер по обеспечению информационной безопасности У-ОПК-10 [1] – уметь формировать политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты В-ОПК-10 [1] – владеть принципами формирования политики информационной безопасности организации
ОПК-12 [1] – Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	З-ОПК-12 [1] – знать способы проектирования подсистем и средств обеспечения защиты информации У-ОПК-12 [1] – уметь проектировать подсистемы и средства обеспечения защиты информации, разрабатывать технико-экономическое обоснование соответствующих проектных решений В-ОПК-12 [1] – владеть принципами проектирования подсистем и средств обеспечения защиты информации
ОПК-5 [1] – Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	З-ОПК-5 [1] – знать нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности У-ОПК-5 [1] – уметь применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности В-ОПК-5 [1] – владеть нормативными правовыми актами, нормативными и методическими документами, регламентирующими деятельность по защите информации в сфере профессиональной деятельности

ОПК-8 [1] – Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	З-ОПК-8 [1] – знать различные способы осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов в целях решения профессиональных задач У-ОПК-8 [1] – уметь осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения профессиональных задач В-ОПК-8 [1] – владеть принципами осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов в целях решения профессиональных задач
УК-2 [1] – Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	З-УК-2 [1] – Знать: виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность У-УК-2 [1] – Уметь: проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты решений для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности В-УК-2 [1] – Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
проектно-технологический			
проектирование и разработка систем информационной безопасности	технологии обеспечения информационной безопасности компьютерных систем	ПК-2 [1] - способен проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов *Основание:*	З-ПК-2[1] - знать действующие нормативные и методические документы по проектированию подсистемы безопасности информации ; У-ПК-2[1] - уметь проектировать

		Профессиональный стандарт: 06.032	подсистемы безопасности информации с учетом действующих нормативных и методических документов; В-ПК-2[1] - владеть принципами проектирования подсистемы безопасности информации

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование культуры информационной безопасности (В23)	Использование воспитательного потенциала дисциплин профессионального модуля для формирование базовых навыков информационной безопасности через изучение последствий халатного отношения к работе с информационными системами, базами данных (включая персональные данные), приемах и методах злоумышленников, потенциальном уроне пользователям.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование профессионально значимых установок: не производить, не копировать и не использовать программные и технические средства, не приобретённые на законных основаниях; не нарушать признанные нормы авторского права; не нарушать тайны передачи сообщений, не практиковать вскрытие информационных систем и сетей передачи данных; соблюдать конфиденциальность доверенной информации (В40)	1. Использование воспитательного потенциала дисциплин "Информатика (Основы программирования)", Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры написания и оформления программ, а также привития навыков командной работы за счет использования систем управления проектами и контроля версий. 2.Использование воспитательного потенциала дисциплины "Проектная практика" для формирования культуры решения изобретательских задач, развития логического мышления, путем погружения студентов в научную и инновационную деятельность

		института и вовлечения в проектную работу. 3.Использование воспитательного потенциала профильных дисциплин для формирования навыков цифровой гигиены, а также системности и гибкости мышления, посредством изучения методологических и технологических основ обеспечения информационной безопасности и кибербезопасности при выполнении и защите результатов учебных заданий и лабораторных работ по криптографическим методам защиты информации в компьютерных системах и сетях. 4.Использование воспитательного потенциала дисциплин " "Информатика (Основы программирования)", Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры безопасного программирования посредством тематического акцентирования в содержании дисциплин и учебных заданий. 5.Использование воспитательного потенциала дисциплины "Проектная практика" для формирования системного подхода по обеспечению информационной безопасности и кибербезопасности в различных сферах деятельности посредством исследования и перенятия опыта постановки и решения научно-практических задач организациями-партнерами.

Организационное и правовое обеспечение информационной безопасности

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
	5 Семестр						
1	Первый раздел	1-8			25	КИ-8	З-ОПК-10, У-ОПК-10, В-ОПК-10, З-ОПК-12, У-ОПК-12, В-ОПК-12, З-ОПК-5, У-ОПК-5, В-ОПК-5
2	Второй раздел	9-16			25	КИ-16	З-ОПК-8, У-ОПК-8, В-ОПК-8, З-ПК-2, У-ПК-2, В-ПК-2, З-УК-

							2, У-УК-2, В-УК-2
	Итого за 5 Семестр		32/0/0		50		
	Контрольные мероприятия за 5 Семестр				50	З	З-ОПК-10, У-ОПК-10, В-ОПК-10, З-ОПК-12, У-ОПК-12, В-ОПК-12, З-ОПК-5, У-ОПК-5, В-ОПК-5, З-ОПК-8, У-ОПК-8, В-ОПК-8, З-ПК-2, У-ПК-2, В-ПК-2, З-УК-2, У-УК-2,

							В-УК-2

* – 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.**
	5 Семестр	32	0	0
1-8	**Первый раздел**	16	16	
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	4	
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	8	
7 - 8	**Организация аналитической работы и контроля состояния защиты конфиденциальной информации.** Организация аналитической работы и контроля состояния	Всего аудиторных часов 4 Онлайн	4	

	защиты конфиденциальной информации. Организация ТЗИ. Организация защиты в АС. Организация защиты информации в рамках 187-ФЗ.			
9-16	**Второй раздел**	16	16	
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	8	
		Онлайн		
13 - 16	**Известные хакерские инциденты.** Известные хакерские инциденты. Истории расследования современных компьютерных инцидентов. Организация и проведение служебного расследования. Практика проведения расследования по различным статьям УК РФ.	Всего аудиторных часов		
		8	8	
		Онлайн		

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-10	З-ОПК-10	З, КИ-8
	У-ОПК-10	З, КИ-8
	В-ОПК-10	З, КИ-8
ОПК-12	З-ОПК-12	З, КИ-8
	У-ОПК-12	З, КИ-8
	В-ОПК-12	З, КИ-8
ОПК-5	З-ОПК-5	З, КИ-8
	У-ОПК-5	З, КИ-8
	В-ОПК-5	З, КИ-8
ОПК-8	З-ОПК-8	З, КИ-16
	У-ОПК-8	З, КИ-16
	В-ОПК-8	З, КИ-16
ПК-2	З-ПК-2	З, КИ-16
	У-ПК-2	З, КИ-16
	В-ПК-2	З, КИ-16
УК-2	З-УК-2	З, КИ-16
	У-УК-2	З, КИ-16
	В-УК-2	З, 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:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69			Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала,
60-64		E	

			но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства приведены в Приложении.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

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

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

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

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

Организационное и правовое обеспечение информационной безопасности

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Организационное и правовое обеспечение информационной безопасности