МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. директора полиграфического института
/И.В. Нагорнова/
«30» июня 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Информационная безопасность систем автоматизации»

Направление подготовки

09.03.02 – «Информационные системы и технологии»

Профиль **«Информационные системы автоматизированных комплексов медиаиндустрии»**

Квалификация (степень) выпускника

Бакалавр

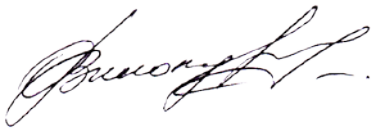
Форма обучения

очная

Москва 2021 г.

Программу составили:

доцент, к.т.н.  /Солонец В.И./

доцент, к.т.н  /Винокурова О.А./

Программа утверждена на заседании кафедры «Полиграфические системы» «23» июня 2021 г., протокол № 11.

Заведующий кафедрой
доц, к. т. н.  /Суслов М.В/

Информационная безопасность систем автоматизации. Прием 2021

1. Цели освоения дисциплины

Целью освоения дисциплины «Информационная безопасность систем автоматизации» является знакомство обучающихся с основными принципами защиты информации в системах полиграфического производства, правовыми законодательными основами защиты информации и интеллектуальной собственности.

Задачами дисциплины является изучение основ защиты информации, видов угроз, правовой базы информационной безопасности.

В результате освоения дисциплины «Информационная безопасность систем автоматизации» обучающийся должен:

Знать: основные положения информационной безопасности компьютерных информационных систем, характеристики уязвимостей промышленных систем, классификацию вредоносного программного обеспечения, основы законодательной базы по вопросам информационной безопасности, основные положения криптографической защиты.

Уметь: использовать правовые документы для оценки правомерности тех или иных действий; выделить типы информации и сформулировать требования к формам защиты; разрабатывать ограничивающую политику безопасности разного уровня.

Владеть: современной программно-информационной средой для решения задач профессиональной деятельности, способностью анализировать данные, полученные в глобальных компьютерных сетях, информационно-коммуникационными технологиями с учетом основных требований информационной безопасности и защиты информации.

Дисциплина способствует подготовке бакалавра к выполнению профессиональных задач в соответствии с проектно-конструкторской деятельностью.

Настоящая дисциплина является дисциплиной обязательной части учебного плана профиля 09.03.02 «Информационные системы автоматизированных комплексов медиаиндустрии» подготовки бакалавров и является одной из дисциплин, завершающих подготовку специалистов этого направления.

2. Место дисциплины в структуре ОП бакалавриата

Дисциплина «Информационная безопасность систем автоматизации» относится к дисциплинам обязательной части учебного плана профиля 09.03.02 «Информационные системы автоматизированных комплексов медиаиндустрии» подготовки бакалавров. Дисциплина взаимосвязана логически и содержательно-методически дисциплинами и практиками образовательной программы направления подготовки 09.03.02 «Информационные системы и технологии» (профиль «Информационные системы автоматизированных комплексов медиаиндустрии»).

Изучение данной дисциплины базируется на следующих дисциплинах учебного плана профиля 09.03.02 «Информационные системы автоматизированных комплексов медиаиндустрии» подготовки бакалавров:

- Операционные системы,
- Введение в программирование
- Интеллектуальные системы и технологии,
- Базы данных

Для освоения учебной дисциплины, обучающиеся должны владеть следующими знаниями и навыками:

- иметь навыки компьютерной грамотности,
- иметь навыки работы с текстовыми редакторами, вычислительными программными средствами.
- иметь навыки работы в глобальных сетях,
- иметь навыки поиска и получения требуемой информации в поисково-информационных системах,

- иметь навыки в использовании информационных технологий для поиска информации с целью решения профессиональных задач.

Полученные умения и навыки могут быть использованы в процессе преддипломной практики и выполнения выпускной квалификационной работы.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины «Информационная безопасность систем автоматизации» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Коды компетенции	Результаты освоения ООП Содержание компетенций*	Перечень планируемых результатов обучения по дисциплине**
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	ИОПК-6.1. Решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий

***** - *формулировка компетенции приводится в соответствии со стандартом.*

** - *характеристика компетенции* (*знать, уметь, владеть*)

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц (216 часов), в том числе самостоятельная работа студента в объёме 148 часов для заочной формы обучения. Изучение дисциплины происходит в течение одного (десятого) семестра. Лекционные занятия планируются в объеме 12 часов, лабораторные занятия – в объеме 20 часов, при этом на подготовку к семестровой аттестации (экзамену) отводится 36 часов.

Трудоемкость по формам обучения:

Форма обучения	**курс**	**семестр**	**Трудоемкость дисциплины в часах**							**Форма контроля**
			Всего час./ зач. ед	**Аудиторных часов (контактная работа)**	**Лекции**	**Семинарские (практические) занятия**	**Лабораторные работы**	**Самостоятельная работа**	**Контроль (промежуточная аттестация)**	
Очная	3	6	144/4	72	36	36		72	-	зачет

Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	семестр
		6
Аудиторные занятия (всего)	72	32
В том числе:		
Лекции	36	36
Практические занятия (ПЗ)	36	36

Семинары (С)		
Лабораторные работы (ЛР)		
Самостоятельная работа (всего)	72	72
В том числе:		
Курсовой проект (работа)		
Расчетно-графические работы		
Реферат	4	4
Другие виды самостоятельной работы		
Домашнее задание		
Вид промежуточной аттестации (зачет, экзамен)	Зачет	зачет
Общая трудоемкость часы	144	144
зачетные единицы	4	4

Структура и содержание дисциплины «Информационная безопасность систем автоматизации» по срокам и видам работы отражены в Приложении 1.

Содержание разделов дисциплины

Тема 1. Введение. Общие вопросы информационной безопасности.

Понятия информации, информатизации, информационной системы, информационной безопасности. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации.

Тема 2. Государственная система информационной безопасности.

Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности.

Тема 3. Угрозы безопасности. Вредоносные программные продукты.

Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы).

Тема 4. Теоретические основы методов защиты информационных систем.

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности.

Тема 5. Методы защиты средств вычислительной техники.

Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от несанкционированного доступа.

Тема 6. Основы криптографии.

Криптография. Основные определения и алгоритмы. Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи.

Тема 7. Архитектура защищенных экономических систем.

Основные технологии построения защищенных экономических информационных систем. Функции защиты информации. Классы задач защиты информации. Архитектура систем защиты информации.

Тема 8. Алгоритмы привязки программного обеспечения к аппаратному окружению.

Индивидуальные параметры вычислительной системы. Блок проверки аппаратного окружения. Дискета как средство привязки. Технология HASP, эмуляторы.

Тема 9. Алгоритмы реализации безопасности в корпоративных сетях.

Понятие корпоративных сетей, структура сети организации, организация хранения информации в ИС; организация обработки информации; регламентация допуска персонала к той или иной информации; ответственность персонала за обеспечение безопасности.

5. Образовательные технологии

Методика преподавания дисциплины и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих форм проведения групповых, индивидуальных, контактных (аудиторных) занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- проведение занятий лекционного типа;
- подготовка к выполнению лабораторно-практических работ в лабораториях и компьютерных классах вуза;
- защита лабораторных работ;
- подготовка информационного доклада по одной из тем.
- контрольная работа.

При проведении лекционных, лабораторных и практических занятий, промежуточной и семестровой аттестации по дисциплине целесообразно использовать следующие образовательные технологии:

1. Процедуры промежуточного контроля по дисциплине «Информационная безопасность систем автоматизации» допускается проводить в форме опроса по теоретической части перед выполнением лабораторных работ и подготовки доклада.

2. В течение семестра в рамках самостоятельной работы обучающиеся выполняют индивидуальные задания, состоящее из теоретической и практической частей.

3. Проведение лекционных занятий, содержащих таблицы и рисунки в качестве иллюстраций, необходимо осуществлять с использованием слайдов, подготовленных в программе Microsoft Power Point.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов: оценочные средства текущего контроля успеваемости и промежуточных аттестаций, подготовка к выполнению лабораторных работ и их выполнение оформление отчета.

Оценочные средства текущего контроля успеваемости включают контрольные вопросы для оперативного опроса и индивидуальные задания для контроля освоения обучающимися разделов дисциплины, защиты лабораторных работ, решение контрольных индивидуальных заданий.

Образцы средств для проведения текущего контроля, экзаменационных билетов, приведены в приложении 2.

Конкретные формы текущего контроля успеваемости по разделам дисциплины приведены в содержании приложения 2.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

В результате освоения дисциплины «Информационная безопасность систем автоматизации» формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОПК-3	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса. Дисциплина «Информационная безопасность систем автоматизации» участвует в формировании перечисленных компетенций.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины, описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

Показатель	Критерии оценивания			
	2	3	4	5
ОПК-3 – способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий				
ИОПК-3.1. Организует работу с технической документацией с учётом основных требований информационной безопасности ИОПК-3.2. Формирует техническую документацию на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие ИОПК-3.1, 3.2	Обучающийся демонстрирует неполное соответствие ИОПК-3.1,3.2 Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие ИОПК-3.1,3.2 Допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие ИОПК-3.1,3.2 Свободно оперирует приобретенными знаниями.

6.1.3 Шкалы оценивания результатов промежуточной аттестации и их описание

Во время лекционных занятий преподаватель отмечает посещаемость по шкале «Да/Нет».

Во время лабораторных занятий преподаватель оценивает активность студента, учитывая самостоятельность выполнения работы, защиту лабораторных работ и сдачу отчетов по ним в указанные сроки.

Шкала оценки работы студента на лабораторном занятии следующая:

- Неудовлетворительно - обучающийся не работал в течение занятия, или отсутствовал,
- Удовлетворительно - обучающийся не смог правильно объяснить решение задания, выполнил не все запланированные задания,
- Хорошо - обучающийся, работая активно, выполнил не все запланированные задания,
- Отлично - обучающийся выполнил все задания и правильно отвечал на поставленные по заданиям вопросы.

Устный опрос (контрольные точки) по текущей теме лабораторной работы проводится во время лабораторных занятий в виде собеседования.

Оценивается:

«максимум» – 3 балла, «минимум» – 2 балла, «неудовлетворительно» – менее 2 баллов.

«максимум»: обучающийся четко и без ошибок или с корректирующими замечаниями преподавателя ответил на все контрольные вопросы по теме лабораторной работы (задачи, индивидуального задания).

«минимум»: обучающийся ответил на все контрольные вопросы по теме лабораторной работы (задачи, индивидуального задания).

«неудовлетворительно»: обучающийся ответил на контрольные вопросы по теме практического задания (задачи, индивидуального задания) с ошибками или не ответил на контрольные вопросы.

Фонд и образцы оценочных средств представлены в приложении 2 к рабочей программе дисциплины.

Промежуточная аттестация обучающихся в форме зачёта проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине, при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине проводится преподавателем, ведущим занятия по дисциплине методом экспертной оценки. По итогам промежуточной аттестации по дисциплине выставляется оценка «зачтено» или «не зачтено».

К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине.

Шкала	Описание

оценивания	
Зачтено	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Не зачтено	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонд и образцы оценочных средств представлены в приложении 2 к рабочей программе дисциплины.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. **Кияев, В., Граничкин, О.** Безопасность информационных систем: курс.- М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с. – URL: http://www.knigafund.ru/books/177798

2. **Мейволд, Э.** Безопасность сетей / Э. Мейволд. – М.: Национальный Открытый Университет «ИНТУМТ», 2016. – 572 с. – URL: http://www.knigafund.ru/books/176437

3. **Загинайлов, Ю.Н.** Теория информационной безопасности и методология защиты информации: учебное пособие. – М.-Берлин: Директ-Медиа, 2015. – 253 с. – URL: http://www.knigafund.ru/books/181420

4. **Шаньгин, В.Ф.** Информационная безопасность и защита информации / В.Ф. Шаньгин. – М. : ДМК Пресс, 2014. – 702 с. : ил.

7.2. Дополнительная литература

1. **Сердюк, В.А.** Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. – М.: Изд. дом Высшей школы экономики, 2015. – 574 с. – URL: http://www.knigafund.ru/books/211708

2. **Мельников, Д.А.** Информационная безопасность открытых систем : учебник для студентов, обучающихся по направлению "Прикладная информатика" / Д.А. Мельников. - М. : ФЛИНТА: Наука, 2013. – 448 с.

3. **Шаньгин, В.Ф.** Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. – М. : ИД "ФОРУМ": ИНФРА-М, 2010. – 591 с.

4. Защита информации с использованием механизмов электронной цифровой подписи : учебно-метод. пособие / Д.Г. Демидов, О.Г. Швечкова, О.А. Москвитина, А.Н. Пылькин, К.А. Майков, К.Г. Смирнова ; Моск. гос. ун-т печати имени Ивана Федорова. – М. : МГУП имени Ивана Федорова, 2014. – 53 с. [Электронный ресурс] URL: http://elib.mgup.ru/showBook.php?id=99

5. **Галатенко В.А.** Основы информационной безопасности: Курс лекций: учебное пособие. - Интернет-Университет Информационных Технологий, 2006. - 208 с. [Электронный ресурс] URL: http://biblioclub.ru/index.php?page=book_red&id=233063&sr=1

6. **Галатенко В.А.** Стандарты информационной безопасности. - Интернет-Университет Информационных Технологий, 2006. - 264 с. [Электронный ресурс] URL: http://biblioclub.ru/index.php?page=book_red&id=233063&sr=1

7.3. Программное обеспечение и Интернет-ресурсы

Для успешного освоения дисциплины, обучающийся использует следующие программные средства: Интернет-браузер FireFox. Лицензия Мосполитеха; LibreOffice 5.0 Бесплатная версия; Adobe Acrobat Reader.

Устойчивый доступ в сеть Internet.

1. Мультимедийные лекции по курсу «Информационная безопасность систем автоматизации».
2. КонсультантПлюс. Надежная правовая поддержка. [Электронный ресурс]. Режим доступа: http://www.consultant.ru/
3. Информационно-правовой портал [Электронный ресурс]. Режим доступа: http://base.garant.ru/
4. Электронный фонд правовой и научно технической документации. [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/
5. Федеральный закон «Об электронной цифровой подписи» от 06.04.2011 N 63-ФЗ (последняя редакция). [Электронный ресурс]. Режим доступа:
   http://www.consultant.ru/document/cons_doc_LAW_112701/
6. Федеральный закон «О коммерческой тайне» от 29.07.04 г. №98-ФЗ // Собрание законодательства Российской Федерации. 2004. № 32. т.3283. (последняя редакция). [Электронный ресурс]. Режим доступа:
   http://www.consultant.ru/document/cons_doc_LAW_48699/
7. Федеральный закон РФ «Об архивном деле в Российской Федерации» от 22 .10. 2004 . Федеральный закон от 22 октября 2004 г. N 125-ФЗ "Об архивном деле в Российской Федерации" Ст. 4169. (с изменениями и дополнениями). [Электронный ресурс]. Режим доступа: http://base.garant.ru/12137300/
8. Федеральный Закон от 13.03. 2006 . № 38–ФЗ «О рекламе» // Собрание Законодательства Российской Федерации. 2006. № 12. Ст. 1232. [Электронный ресурс]. Режим доступа:
   http://ipipip.ru/zakon-o-reklame/
   http://logos-pravo.ru/zakon-o-reklame-no-38-fz
9. Федеральный Закон от 27.07. 2006 . № 149–ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание Законодательства Российской Федерации. 2006. № 31. (Ч. 1). Ст. 3448. [Электронный ресурс]. Режим доступа:
   http://www.consultant.ru/document/cons_doc_LAW_61798/
10. Федеральный Закон от 27.07. 2006 . № 152–ФЗ «О персональных данных» // Собрание Законодательства Российской Федерации. 2006. № 31. (Ч. 1). Ст. 3451. [Электронный ресурс]. Режим доступа: http://base.garant.ru/12148567/

11. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования. [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/1200007350
12. ГОСТ Р 50922-96. Защита информации: Основные термины и определения. [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/1200004674
13. ГОСТ 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/1200025597
14. CIT Forum. URL: http://www.citforum.ru (дата обращения 12.06.2011).
15. Журнал «Защита информации. Инсайд». URL: https://www.inside-zi.ru/
16. InformationSecurity: Информационная безопасность. URL: http://www.itsec.ru/main.php
17. Информационная безопасность. URL: https://securityvulns.ru/

8. Материально-техническое обеспечение дисциплины

1. Аудитории Пр 2806, Пр2808, Пр2810, Пр2845Б (компьютерный класс не менее 10-15 посадочных мест) с установленным программным обеспечением для проведения лабораторно-практических занятий.
2. Комплекс технических средств, позволяющих проецировать изображение из программных средств подготовки презентаций (экран, проектор, ноутбук или компьютер с подключенным оборудованием, интерактивная доска).
3. Возможность доступа в интернет.

9. Методические рекомендации для самостоятельной работы студентов

Учебным планом предусмотрено изучение дисциплины «Информационная безопасность систем автоматизации» в 10 семестре при заочной форме обучения. По дисциплине проводятся лекционные и лабораторные занятия.

Лекционные занятия проводятся в соответствии с содержанием настоящей рабочей программы и представляют собой изложение основ информационной безопасности, основ построения государственной системы информационной безопасности, законодательной базы, информации о вредоносных программных продуктах, о методах защиты информационных систем, средств вычислительной техники, экономических систем, компьютерных сетей, о криптографических методах защиты.

Посещение лекционных занятий является обязательным. Допускается конспектирование лекционного материала как письменным, так и компьютерным способом.

Регулярная проработка материала конспектов лекций по каждому разделу в рамках подготовки к промежуточным и семестровым формам аттестации по дисциплине «Информационная безопасность систем автоматизации» является одним из важнейших видов самостоятельной работы обучающегося в течение семестра, необходимой для качественной подготовки к промежуточной и семестровой аттестации по дисциплине.

Семестровая аттестация по дисциплине проходит в форме экзамена. Экзаменационный билет по дисциплине «Информационная безопасность систем автоматизации» состоит из вопросов теоретического характера и практического задания (задачи). Примерный перечень вопросов к экзамену по дисциплине «Информационная безопасность систем автоматизации» приведен в приложении 2 к настоящей рабочей программе, а критерии оценки ответа студента на экзамене – в п. 6 настоящей рабочей программы.

10. Методические рекомендации для преподавателя

Дисциплина «Информационная безопасность систем автоматизации» является дисциплиной обязательной части учебного плана.

Преподавание теоретического (лекционного) материала по дисциплине «Информационная безопасность систем автоматизации» осуществляется по последовательной схеме на основе образовательной программы и учебного плана по направлению 09.03.02 – «Информационные системы и технологии», профиля «Информационные системы автоматизированных комплексов медиаиндустрии».

Рекомендуемые образовательные технологии: лекции и лабораторные занятия, самостоятельная работа студентов (в том числе выполнение индивидуального задания), выполнение контрольных (самостоятельных) работ, подготовка докладов.

Подробное содержание отдельных разделов дисциплины «Информационная безопасность систем автоматизации» представлено в п. 4 рабочей программы.

Структура и последовательность проведения лабораторных занятий по дисциплине представлены в приложении 1 к настоящей рабочей программе.

Целесообразные к применению в рамках дисциплины «Информационная безопасность систем автоматизации» образовательные технологии изложены в п.10 настоящей рабочей программы.

Примерные варианты заданий для промежуточного/семестрового контроля и перечень вопросов к экзамену по дисциплине представлены в соответствующих подпунктах приложения 2 к рабочей программе.

Перечень основной и дополнительной литературы и нормативных документов, необходимых в ходе преподавания дисциплины «Информационная безопасность систем автоматизации», приведен в п. 7 настоящей рабочей программы. Преподавателю следует ориентировать обучающихся на использование при подготовке к промежуточной и семестровой аттестации по дисциплине материалов лекций.

При проведении занятий рекомендуется использование активных аудиторных занятий в сочетании с внеаудиторной работой, в том числе выполнение индивидуальных заданий и подготовка доклада по одной из тем.

Программа составлена в соответствии с:

- Образовательной программой направления 09.03.02 «Информационные системы и технологии», профиля «Информационные системы автоматизированных комплексов медиаиндустрии».

Приложение 1

Структура и содержание дисциплины «Информационная безопасность систем автоматизации»
по направлению подготовки по направлению подготовки 09.03.02
«Информационные системы и технологии»
(бакалавр)

1.1. Тематический план дисциплины

№ п/п	Наименование раздела дисциплины	Лекции	Практические занятия	СРС	Всего
1.	Тема 1. Общие вопросы информационной безопасности	4	2	8	14
2.	Тема 2. Государственная система информационной безопасности	4	4	8	16
3.	Тема 3. Угрозы безопасности. Вредоносные программные продукты	4	6	8	18
4.	Тема 4. Теоретические основы методов защиты информационных систем	4	4	8	16
5.	Тема 5. Методы защиты средств вычислительной техники.	4	4	8	16
6.	Тема 6. Основы криптографии	4	6	8	18
7.	Тема 7. Архитектура защищенных экономических систем	4	2	8	16
8.	Тема 8. Алгоритмы привязки программного обеспечения к аппаратному окружению	4	4	8	16
9.	Тема 9. Алгоритмы реализации безопасности в корпоративных сетях	4	4	8	16
	Итого	36	36	72	144

1.2. Лабораторный практикум (не предусмотрены)

1.3. Практические занятия

№ п/п	№ раздела дисциплины	Наименование лабораторных занятий	Трудоемкость
1.	Тема 1.	*работа 1.* Информационный поиск и обзор на тему «Структура законодательной базы по вопросам информационной безопасности».	2
2.	Тема 2.	*работа 2.* Информационный поиск и обзор на тему «Структура государственной системы информационной безопасности».	4
3.	Тема 3.	*работа 3.* Анализ и классификация угроз безопасности.	6
4.	Тема 4.	*работа 4.* Оценка информационных потоков. Выделение типов информации, формирование требований защиты информации.	4
5.	Тема 5	*работа 5.* Методы защиты средств вычислительной техники. Разработка ограничивающих политик безопасности на уровне политик компьютеров, политик пользователей, политик учетных записей.	2
6.	Тема 5.	*работа 6.* Изучение средств защиты информации в Windows.	2
7.	Тема 6.	*работа 7.* Основы криптографии. Изучение криптографических	2

		методов шифрования (перестановки, подстановки)	
8.	Тема 6	*работа 8.* Особенности методов шифрования с открытым ключом	2
9.	Тема 6	*работа 9.* Криптосистемы на основе эллиптических уравнений	2
10.	Тема 7	*работа 10.*Архитектура систем	2
11.	Тема 8	*работа 11.* Алгоритмы привязки ПО	4
12.	Тема 9	*работа 12.* Реализация сетевых алгоритмов безопасности	4

Приложение 2.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 09.03.02 – «Информационные системы и технологии»

ОП (профиль): «Информационные системы автоматизированных комплексов медиаиндустрии»

Форма обучения: очная

Вид профессиональной деятельности: производственно-технологическая

Кафедра «Полиграфические системы

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

«Информационная безопасность систем автоматизации»

Состав:

1. Паспорт фонда оценочных средств
2. Показатель сформированности компетенций
3. Примерный перечень оценочных средств
4. Описание оценочных средств (образцы тестовых заданий, контрольных и экзаменационных вопросов по курсу «Информационная безопасность систем автоматизации»)

Составители: доцент, к.т.н. Винокурова О.А., доцент, к.т.н. Солонец В.И.

Москва 2021 г.

П2.1 Паспорт фонда оценочных средств по дисциплине «Информационная безопасность систем автоматизации»

№ п/п	Контролируемые разделы дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1.	Тема 1. Общие вопросы информационной безопасности	ОПК-3	УО К/Р ДС Э
2.	Тема 2. Государственная система информационной безопасности	ОПК-3	УО К/Р ОЛР ДС Э
3.	Тема 3. Угрозы безопасности. Вредоносные программные продукты	ОПК-3	УО К/Р ДС Э
4.	Тема 4. Теоретические основы методов защиты информационных систем	ОПК-3	УО К/Р ОЛР ДС Э
5.	Тема 5. Методы защиты средств вычислительной техники	ОПК-3	УО К/Р ОЛР ДС Э
6.	Тема 6. Основы криптографии	ОПК-3	УО К/Р ОЛР ДС Э
7.	Тема 7. Архитектура защищенных экономических систем	ОПК-3	УО К/Р ДС Э
8.	Тема 8. Алгоритмы привязки программного обеспечения к аппаратному окружению	ОПК-3	УО К/Р ДС Э
9.	Тема 9. Алгоритмы реализации безопасности в компьютерных сетях	ОПК-3	УО К/Р ДС Э

П2.2. Показатель уровня сформированности компетенций

Дисциплина «Информационная безопасность систем автоматизации»

ФГОС ВО **09.03.02 – «Информационные системы и технологии»**

В процессе освоения данной дисциплины обучающийся формирует и демонстрирует следующие компетенции

Компетенции		**Перечень индикаторов достижения компетенции**	**Технология формирования компетенций**	**Форма оценочного средства****	**Степени уровней освоения компетенций**
индекс	**формулировка**				
ОПК-6	способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	ИОПК-3.1. Организует работу с технической документацией с учётом основных требований информационной безопасности ИОПК-3.2. Формирует техническую документацию на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	Лекция Лабораторная работа Самостоятельная работа	УО К/Р ОЛР ДС Э	• знает основы законодательной базы по вопросам информационной безопасности, • знает характеристики уязвимостей промышленных систем, • знает классификацию вредоносного программного обеспечения, угроз безопасности, • знает основы криптографической защиты, • умеет использовать правовые документы для оценки правомерности тех или иных действий, • владеет информационно-коммуникационными технологиями с учетом основных требований информационной безопасности автоматизированных технологических процессов и производств, • владеет методами анализа информации и выбора наиболее подходящего варианта информационной защиты систем автоматизации.

** - Сокращения форм оценочных средств см. в приложении П2.3 к РП.

П2.3 Примерный перечень оценочных средств (ОС) по дисциплине Информационная безопасность систем автоматизации

№ ОС	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1.	Устный опрос собеседование, (УО)	Средство контроля, организованное как специальная беседа педагогического работника с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
2.	Контрольная работа (К/Р)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу	Комплект контрольных заданий по вариантам
3.	Отчет по лабораторной работе (ОЛР)	Продукт самостоятельной работы обучающегося, представляющий собой средство проверки умений применять полученные знания для решения поставленной задачи по заранее определенной методике и краткое изложение в письменном виде полученных результатов экспериментального и теоретического анализа определенной учебно- исследовательской темы.	Перечень и темы лабораторных работ
4.	Доклад, сообщение (ДС)	Продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно- практической, учебно-исследовательской или научной темы	Темы докладов, сообщений
5.	Экзамен (Э)	Форма промежуточной аттестации студента, определяемые учебным планом подготовки по направлению	Комплект экзаменационных билетов

П2.4. Описание оценочных средств по дисциплине «Информационная безопасность систем автоматизации»

П2.4.1 Контрольные вопросы по дисциплине «Информационная безопасность систем автоматизации»

Приведённый ниже перечень контрольных вопросов используется в качестве вопросов экзаменационных билетов, а также при устном опросе обучающихся и в качестве дополнительных вопросов при защите лабораторных работ.

1. Определить место информационной безопасности в обеспечении системы общественной безопасности.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной безопасности общества.
4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
5. Охарактеризовать уровни реализации информационной безопасности.
6. Дать определение и классификацию информационных ресурсов.
7. Определить основные виды угроз информационным ресурсам.
8. Охарактеризовать особенности угроз конфиденциальной информации.
9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
10. Описать причины возникновения каналов несанкционированного доступа к информации.
11. Классифицировать виды каналов несанкционированного доступа к информации.
12. Описать характер действия организационных каналов несанкционированного доступа к информации.
13. Охарактеризовать технические каналы несанкционированного доступа к информации.
14. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.
15. Проанализировать особенности угроз автоматизированным информационным системам.
16. Дать классификацию удаленных атак.
17. Проанализировать основные направления правовой защиты информации.
18. Раскрыть содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.
19. Изложить законный порядок реализации права гражданина на опровержение ложной информации о нем в средствах массовой информации.
20. Показать порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.
21. Определить объекты защиты авторских прав.
22. Назвать основные права автора в отношении его произведения.
23. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.
24. Охарактеризовать основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).
25. Дать определение государственной тайны и назвать грифы секретности.
26. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.
27. Изложить порядок отнесения сведений к государственной тайне и их засекречивания.
28. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне.

29. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.
30. Охарактеризовать порядок установления режима коммерческой тайны и основные права ее субъектов.
31. Назвать основные виды служебной тайны определенные законодательством Российской Федерации.
32. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.
33. Назвать основные положения концепции информационной безопасности предприятия.
34. Изложить содержание регламента обеспечения информационной безопасности предприятия.
35. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.
36. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.
37. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.
38. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.
39. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.
40. Проанализировать особенности контроля исполнения конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.
41. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.
42. Проанализировать особенности текста конфиденциального документа.
43. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.
44. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.
45. Сформулировать возможности, трудности и направления использования электронной почты для передачи конфиденциальных документов.
46. Составить фрагмент номенклатуры дел, содержащих конфиденциальные документы.
47. Проанализировать задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами.
48. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.
49. Проанализировать пути поиска документов и дел, не обнаруженных при проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.
50. Составить и проанализировать технологическую схему (цепочку) приема (перевода) лиц на работу, связанную с владением конфиденциальной информацией.
51. Составить и проанализировать технологическую схему (цепочку) увольнения сотрудников, владеющих конфиденциальной информацией.
52. Проанализировать виды угроз безопасности конфиденциальной информации фирмы при демонстрации на выставке новой продукции.
53. Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализировать степень опасности каждого канала.

54. Назвать основные элементы физической защиты территории и помещений предприятия.
55. Охарактеризовать способы и элементы программно-технической защиты информационных ресурсов.
56. Дать классификацию компьютерных вирусов.
57. Описать основные антивирусные программы.
58. Охарактеризовать основные способы криптографического преобразования данных.

П2.4.2. Примерные варианты задания для контрольных работ по дисциплине «Информационная безопасность систем автоматизации»

Контрольная работа №1:

1. Общая характеристика и классификация Средств защиты ИС. Категориальные понятия системного подхода. Формальные методы описания структуры системы. Понятие архитектуры
2. Категориальные понятия системного подхода.
3. Формальные методы описания структуры системы. Понятие архитектуры.
4. Модели функционирования Средств защиты ИС.
5. Технологии разработки Средств защиты ИС.
6. Особенности реализации Средств защиты ИС в различных предметных областях.

Контрольная работа №2:

1. Модели функционирования Средств защиты ИС.
2. Технологии разработки Средств защиты ИС.
3. Особенности реализации Средств защиты ИС в различных предметных областях.
4. Модели и структуры Средств защиты ИС.
5. Информационные ресурсы. Теоретические основы современных Средств защиты ИС.
6. Базовая эталонная модель Международной организации стандартов.
7. Компоненты Средств защиты ИС

Контрольная работа №3

1. Архитектура Средств защиты ИС в научных исследованиях.
2. Научные исследования, испытания и эксперименты как объект автоматизации.
3. Функциональные задачи автоматизированных систем научных исследований (АСНИ).
4. Классификация АСНИ, обеспечения АСНИ, функциональная и системная архитектуры.
5. Эталонные аппаратные платформы.
6. Типовые архитектурно-структурные решения, используемые при создании Средств защиты ИС.
7. Программное обеспечение Средств защиты ИС.

П2.4.3. Примерная тематика докладов по дисциплине «Информационная безопасность систем автоматизации»

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Основы экономической безопасности предпринимательской деятельности.

4. Анализ законодательных актов об охране информационных ресурсов открытого доступа.
5. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
6. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
7. Информационная безопасность **(**по материалам зарубежных источников и литературы).
8. Правовые основы защиты конфиденциальной информации.
9. Экономические основы защиты конфиденциальной информации.
10. Организационные основы защиты конфиденциальной информации.
11. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.
12. Составление инструкции по обработке и хранению конфиденциальных документов.
13. Направления и методы защиты документов на бумажных носителях.
14. Направления и методы защиты машиночитаемых документов.
15. Архивное хранение конфиденциальных документов.
16. Направления и методы защиты аудио- и визуальных документов.
17. Порядок подбора персонала для работы с конфиденциальной информацией.
18. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.
19. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
20. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
21. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
22. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.
23. Порядок защиты информации в рекламной и выставочной деятельности.
24. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
25. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).
26. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).
28. Назначение, виды, структура и технология функционирования системы защиты информации.
29. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
30. Аналитическая работа по выявлению каналов утечки информации фирмы.
31. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.
32. Направления и методы защиты профессиональной тайны.
33. Направления и методы защиты служебной тайны.
34. Направления и методы защиты персональных данных о гражданах.
35. Методы защиты личной и семейной тайны.
36. Построение и функционирование защищенного документооборота.

37. Защита секретов в дореволюционной России.
38. Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

П2.4.4 Образец экзаменационного билета по дисциплине «Информационная безопасность систем автоматизации ».

министерство науки и высшего образования российской федерации
федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Институт *полиграфический* Кафедра *Полиграфические системы*

Дисциплина *Информационная безопасность систем автоматизации*

Направление подготовки 09.03.02 *Автоматизация технологических процессов и производств*

курс _____ группа _____ Форма обучения *очная*

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № ____

1. Порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.

2. Принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.

3. Основы криптографии. Криптографические методы шифрования.

Утверждено на заседании кафедры ПС

«___» _____20___ г., протокол № _____

Зав. кафедрой _____ /Суслов М.В./