

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 22.08.2025 10:52:18
Уникальный программный ключ:
b683afe664d7e9f64175886cf9626a196149ad36

СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет Математики и информационных технологий
Кафедра Математического моделирования

Аннотация рабочей программы дисциплины (модуля)

дисциплина **Системы защиты информации в зарубежных странах**

Блок Б1, базовая часть, Б1.Б.35

цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

10.03.01

Информационная безопасность

код

наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очная

Для поступивших на обучение в
2020 г.

1. Перечень планируемых результатов обучения по дисциплине (модулю)

1.1. Перечень планируемых результатов освоения образовательной программы

Выпускник, освоивший программу высшего образования, в рамках изучаемой дисциплины, должен обладать компетенциями, соответствующими видам профессиональной деятельности, на которые ориентирована программа:

Способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7)

Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Формируемая компетенция (с указанием кода)	Этапы формирования компетенции	Планируемые результаты обучения по дисциплине (модулю)
Способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7)	1 этап: Знания	Обучающийся должен знать: - состав защищаемой информации на различных этапах развития зарубежных стран, её классификацию; - состав, структуру и основные направления деятельности органов защиты информации; - состав, особенности классификации, структуру угроз защищаемой информации в различные исторические периоды и на современном этапе.
	2 этап: Умения	Обучающийся должен уметь: - разграничивать угрозы, опасности, их источники, а также функции и сферы деятельности различных органов, действующих в сфере обеспечения национальной безопасности; - давать оценку организационно-правовому состоянию защиты информации на разных этапах

		развития.
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: - навыками работы с нормативно-правовыми актами в области защиты информации; - понятийным аппаратом в области защиты информации;
Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)	1 этап: Знания	Обучающийся должен знать: - особенности формирования и развития нормативной базы защиты информации в зарубежных странах; - основные направления государственной политики в области защиты информации в ведущих зарубежных странах; - направления и методы защиты информации, факторы, определяющие современную систему защиты информации и тенденции ее развития.
	2 этап: Умения	Обучающийся должен уметь: - применять полученные знания в профессиональной и иной деятельности; - определять и классифицировать возникающие угрозы безопасности и применять свои знания для предупреждения опасных ситуаций.
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: - навыками работы с законодательными и другими нормативными правовыми актами в области защиты информации, принятия правовых решений в соответствии с ними; - навыками выявления и

		анализа угроз информационной безопасности.
--	--	--

2. Место дисциплины (модуля) в структуре образовательной программы

Для изучения учебной дисциплины «Системы защиты информации в зарубежных странах» необходимы знания, умения и навыки, формируемые в процессе изучения дисциплин: «Основы управления информационной безопасностью», «Информационные системы управления производственной компанией», «Организационное и правовое обеспечение информационной безопасности», «Правовые информационные системы», «Техническая защита информации» и других.

Знания, умения и навыки, формируемые дисциплиной «Системы защиты информации в зарубежных странах», необходимы для успешного освоения последующих дисциплин: «Информационная безопасность предприятия», и других, связанных с обработкой информации и ее оформлением в соответствии с профессиональными требованиями, а также прохождения практики и написания выпускной квалификационной работы.

Дисциплина изучается на 4 курсе в 8 семестре

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 4 зач. ед., 144 acad. ч.

Объем дисциплины	Всего часов
	Очная форма обучения
Общая трудоемкость дисциплины	144
Учебных часов на контактную работу с преподавателем:	
лекций	12
практических (семинарских)	18
лабораторных	18
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	34,8
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	60

Формы контроля	Семестры
экзамен	8

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

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№ п/п	Наименование раздела / темы дисциплины	Виды учебных занятий, включая самостоятельную работу обучающихся и
-------	--	--

		трудоемкость (в часах)			
		Контактная работа с преподавателем			СР
		Лек	Пр/Сем	Лаб	
1	Модуль 1	6	10	6	26
1.1	История развития информационной безопасности в зарубежных странах	4	6	2	10
1.2	Информационная безопасность в системе национальной безопасности в зарубежных странах	2	4	4	16
2	Модуль 2	6	8	12	34
2.1	Анализ способов нарушений информационной безопасности. Компьютерные вирусы. Методы криптографии.	4	6	6	18
2.2	Концепции информационной безопасности в зарубежных странах	2	2	6	16
	Итого	12	18	18	60

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Модуль 1	
1.1	История развития информационной безопасности в зарубежных странах	Эволюция информационного противоборства. Генезис развития систем разведки и защиты информации в мировой практике. Становление и этапы развития систем защиты информации в ведущих зарубежных странах с древности и до начала XX века.
1.2	Информационная безопасность в системе национальной безопасности в зарубежных странах	Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз. Информационная война как высшая форма угрозы информационной безопасности.
2	Модуль 2	
2.1	Анализ способов нарушений информационной безопасности. Компьютерные вирусы. Методы криптографии.	Источники дестабилизирующего воздействия на защищаемую информацию как определяющая структурная часть угрозы. Состав и характеристика источников дестабилизирующего воздействия на информацию. Виды и способы дестабилизирующего воздействия на информацию со стороны различных источников. Соотношение видов дестабилизирующего воздействия на защищаемую информацию с формами проявления уязвимости информации.
2.2	Концепции информационной безопасности в зарубежных странах	Понятие и современная концепция национальной безопасности. Концепция охраны объектов. Категорирование объектов охраны. Понятие «система защиты информации».

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Модуль 1	
1.1	История развития информационной безопасности в зарубежных странах	Этапы развития систем защиты информации в ведущих зарубежных странах с древности и до начала XX века. Разработка нормативной базы отдельного государства.
1.2	Информационная безопасность в системе национальной безопасности в зарубежных странах	Программно-аппаратные, криптографические и стенографические средства обеспечения информационной безопасности.
2	Модуль 2	
2.1	Анализ способов нарушений информационной безопасности. Компьютерные вирусы. Методы криптографии.	Особенности утечки информации. Классификация вирусов. Способы заражения программ: метод приписывания, метод оттеснения, метод вытеснения, сохранение вытесненного фрагмента программы в «кластерном хвосте» файла и пр. Виды антивирусных программ: программы-детекторы; программы-доктора или фаги; программы-ревизоры; программы-фильтры; программы-вакцины или иммунизаторы.
2.2	Концепции информационной безопасности в зарубежных странах	Понятие и назначение технологического обеспечения защиты информации. Классификация организационно-технологических документов по защите информации. Классификация мероприятий по защите информации, сферы применения организационно-технологических документов и мероприятий. Значение и виды контрольных мероприятий. Аналитическая работа по предотвращению утраты и утечки информации. Классификация подходов к оценке эффективности систем защиты информации. Вероятностный подход: структуризация предметной области оценки, анализ вероятности реализации угроз безопасности, расчетные соотношения. Оценочный подход на основе формирования требований защищенности объекта: классы защищенности и их характеристика, контрольно-испытательные процедуры определения соответствия защиты установленным требованиям. Содержание и особенности экспертной оценки эффективности защиты.

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Модуль 1	
1.1	История развития информационной безопасности в зарубежных странах	Генезис развития систем разведки и защиты информации в мировой практике. Становление и этапы развития систем защиты информации в ведущих зарубежных странах с древности и до начала XX века.

		Предпосылки формирования системы защиты информации.
1.2	Информационная безопасность в системе национальной безопасности в зарубежных странах	Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. Программно-аппаратные, криптографические и стенографические средства обеспечения информационной безопасности.
2	Модуль 2	
2.1	Анализ способов нарушений информационной безопасности. Компьютерные вирусы. Методы криптографии.	Источники и причины утечки информации. Показатели эффективности добывания информации. Способы и средства добывания информации, наблюдения, перехвата сигналов, подслушивания. Особенности утечки информации. Классификация вирусов по следующим признакам: по среде обитания вируса; по способу заражения среды обитания; по деструктивным возможностям; по особенностям алгоритма вируса. Способы заражения программ: метод приписывания, метод оттеснения, метод вытеснения, сохранение вытесненного фрагмента программы в «кластерном хвосте» файла и пр.
2.2	Концепции информационной безопасности в зарубежных странах	Понятие «система защиты информации». Назначение систем. Классификация систем защиты информации, сферы их действия. Сущность и значение комплексной системы защиты информации как формы организации деятельности по защите информации.