

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 30.10.2023 11:19:52
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

Рабочая программа дисциплины (модуля)

дисциплина ***Б1.О.25 Основы управления информационной безопасностью***

обязательная часть

Направление

10.03.01
код

Информационная безопасность
наименование направления

Программа

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

Форма обучения

Очно-заочная

Для поступивших на обучение в
2023 г.

Разработчик (составитель)
к.ф.-м.н., доцент
Викторов С. В.
ученая степень, должность, ФИО

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций	3
2. Цели и место дисциплины (модуля) в структуре образовательной программы	4
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	4
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий.....	4
4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах).....	4
4.2. Содержание дисциплины, структурированное по разделам (темам)	5
5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю).....	8
6. Учебно-методическое и информационное обеспечение дисциплины (модуля)	8
6.1. Перечень учебной литературы, необходимой для освоения дисциплины (модуля)	8
6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем	9
6.3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства	10
7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)	10

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)
<p>ОПК-10. 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;</p>	<p>ОПК-10.1. Знает меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты.</p>	<p>Обучающийся должен: базовый понятийный аппарат в области информационной безопасности и защиты информации; виды и состав угроз информационной безопасности; принципы и общие методы обеспечения информационной безопасности.</p>
	<p>ОПК-10.2. Способен формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности.</p>	<p>Обучающийся должен: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>
	<p>ОПК-10.3. Владеет навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.</p>	<p>Обучающийся должен: методами и способами выявления угроз информационной безопасности применительно к объектам защиты с учетом содержания информационных процессов и особенностей их функционирования.</p>

2. Цели и место дисциплины (модуля) в структуре образовательной программы

Цели изучения дисциплины:

Цель дисциплины - изучение основных понятий, методологии и применения практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.

Дисциплина реализуется в рамках обязательной части. Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Теория информации», «Основы информационной безопасности».

Дисциплина изучается на 2 курсе в 4 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 6 зач. ед., 216 акад. ч.

Объем дисциплины	Всего часов
	Очно-заочная обучения
Общая трудоемкость дисциплины	216
Учебных часов на контактную работу с преподавателем:	
лекций	24
практических (семинарских)	28
лабораторных	28
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	34,8
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	100

Формы контроля	Семестры
экзамен	4

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	Теоретические основы информационной безопасности	12	14	15	50

1.1	Основные понятия теории информационной безопасности	4	4	0	10
1.2	Информация как объект защиты	4	4	0	15
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	2	4	0	10
1.4	Угрозы информационной безопасности	2	2	15	15
2	Методология защиты информации	12	14	13	50
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	4	4	0	10
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	4	4	0	15
2.3	Политика и модели безопасности	2	4	0	10
2.4	Обзор международных стандартов информационной безопасности	2	2	13	15
	Итого	24	28	28	100

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Теоретические основы информационной безопасности	
1.1	Основные понятия теории информационной безопасности	История становления и предметная область теории информационной безопасности. Систематизация понятий в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации». Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации.
1.2	Информация как объект защиты	Понятие об информации как объекте защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы. Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов.
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	Информационная безопасность и ее место в системе национальной безопасности Российской Федерации. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.

1.4	Угрозы информационной безопасности	Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.
2	Методология защиты информации	
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	Определение и основные способы несанкционированного доступа. Методы защиты от НСД. Организационные методы защиты от НСД. Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Основные направления и цели использования криптографических методов. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	Защита целостности информации при хранении. Защита целостности информации при обработке. Защита целостности информации при транспортировке. Защита от угрозы нарушения целостности информации на уровне содержания. Построение систем защиты от угрозы отказа доступа к информации. Защита семантического анализа и актуальности информации.
2.3	Политика и модели безопасности	Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения доступа. Политика и модели мандатного доступа. Теоретико-информационные модели. Политика и модели тематического разграничения доступа. Ролевая модель безопасности
2.4	Обзор международных стандартов информационной безопасности	Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности

		информационных технологий США. Единые критерии безопасности информационных технологий.
--	--	---

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Теоретические основы информационной безопасности	
1.4	Угрозы информационной безопасности	Выбор мер защиты информации для автоматизированного рабочего места
2	Методология защиты информации	
2.4	Обзор международных стандартов информационной безопасности	Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000 на разных устройствах.

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Теоретические основы информационной безопасности	
1.1	Основные понятия теории информационной безопасности	Систематизация понятий в области защиты информации. Основные термины и определения понятий в области информационной защиты информации. Принципы построения систем защиты. Задачи защиты информации. Средства реализации комплексной защиты информации.
1.2	Информация как объект защиты	Уровни представления информации. Виды и формы представления информации. Свойства защищаемой информации. Структура и шкала ценности информации. Классификация информационных ресурсов.
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	Роль и место информационной безопасности в системе национальной безопасности РФ. Нормативная деятельность, функции и задачи органов обеспечения информационной безопасности и защиты информации.
1.4	Угрозы информационной безопасности	Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.

2	Методология защиты информации	
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	Методы защиты от несанкционированного доступа. Организационные и инженерно-технические методы защиты от несанкционированного доступа. Построение систем защиты от угрозы утечки по техническим каналам. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности информации.
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	Защита целостности информации при хранении, обработке, транспортировке. Построение систем защиты от угрозы отказа доступа к информации. Семантический анализ.
2.3	Политика и модели безопасности	Модели разграничения доступа в рамках политики безопасности. Модели дискреционного доступа. Парольные системы разграничения доступа. Модели тематического разграничения доступа.
2.4	Обзор международных стандартов информационной безопасности	Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000.

5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю)

Наименование тем на самостоятельное изучение:

1. Информационные войны и информационное противоборство.
2. Определение и основные виды информационных войн
3. Информационно-техническая война.
4. Информационно-психологическая война.

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1. Перечень учебной литературы, необходимой для освоения дисциплины (модуля)

Основная учебная литература:

1. 1. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=562348> (дата обращения: 20.06.2021).
2. 2. Гультаева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гультаева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=574729> (дата обращения: 20.06.2021).
3. 3. Загинайлов, Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 105 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=362895> (дата обращения: 20.06.2021).

Дополнительная учебная литература:

1. 1. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=562348> (дата обращения: 25.05.2023).
2. 2. Основы информационной безопасности: учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – Москва : Горячая линия – Телеком, 2011. – 558 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=253056> (дата обращения: 25.05.2023).

6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем

№ п/п	Наименование документа с указанием реквизитов
1	Договор на доступ к ЭБС ZNANIUM.COM между БашГУ в лице директора СФ БашГУ и ООО «Знаниум» № 3/22-эбс от 05.07.2022
2	Договор на доступ к ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между БашГУ в лице директора СФ БашГУ и ООО «Электронное издательство ЮРАЙТ» № 1/22-эбс от 04.03.2022
3	Договор на доступ к ЭБС «Университетская библиотека онлайн» между БашГУ и «Нексмедиа» № 223-950 от 05.09.2022
4	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-948 от 05.09.2022
5	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-949 от 05.09.2022
6	Соглашение о сотрудничестве между БашГУ и издательством «Лань» № 5 от 05.09.2022
7	ЭБС «ЭБ БашГУ», бессрочный договор между БашГУ и ООО «Открытые библиотечные системы» № 095 от 01.09.2014 г.
8	Договор на БД диссертаций между БашГУ и РГБ № 223-796 от 27.07.2022
9	Договор о подключении к НЭБ и о предоставлении доступа к объектам НЭБ между БашГУ в лице директора СФ БашГУ с ФГБУ «РГБ» № 101/НЭБ/1438-П от 11.06.2019
10	Договор на доступ к ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между УУНиТ в лице директора СФ УУНиТ и ООО «Электронное издательство ЮРАЙТ» № 1/23-эбс от

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»)

№ п/п	Адрес (URL)	Описание страницы
1	http://internetsecure.ru/	Набор технологий и программ для безопасной работы в сети с компьютером
2	http://www.content-filtering.ru/	Интернет- СМИ "Ваш личный Интернет" - помощь родителям в организации безопасного доступа детей в сеть Интернет
3	https://securelist.ru/enciklopediya	Энциклопедия информационной безопасности
4	http://www.securitylab.ru/software/1423/	Каталог программ «Защита детей от интернет угроз» (описание, сравнение, оценки)
5	http://www.oszone.net/6213/	Обеспечение безопасности детей при работе в Интернет (статья, ссылки, материалы)
6	http://www.securityportal.ru/	Сайт по защите информации, защите приватности, безопасным сетевым взаимодействиям, криптографии.
7	http://www.anti-malware.ru/	Независимый информационно-аналитический портал по безопасности

6.3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование программного обеспечения
Kaspersky Endpoint Security
Office Standart 2007 Russian OpenLicensePack NoLevel Acdmc
Windows XP

7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Тип учебной аудитории	Оснащенность учебной аудитории
Лаборатория технической защиты информации. Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных	Доска, проектор, экран, учебная мебель, компьютеры, учебно-наглядные пособия.

консультаций	
Лаборатория программно-аппаратных средств обеспечения информационной безопасности. Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций.	Доска, проектор, экран, учебная мебель, компьютеры, учебно-наглядные пособия.
Лаборатория электричества и магнетизма. Учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций.	Доска, учебная мебель, оборудование для проведения лабораторных работ.
Читальный зал: помещение для самостоятельной работы.	Учебная мебель, учебно-наглядные пособия, компьютеры с доступом к сети «Интернет» и ЭИОС Филиала.
Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций.	Доска, учебная мебель, проектор, экран, учебно-наглядные пособия.