

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 22.08.2025 10:48:46
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 ***Теоретические основы защиты информации***

Блок Б1, базовая часть, Б1.Б.25

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.

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

1. Перечень планируемых результатов обучения по дисциплине (модулю)	3
1.1. Перечень планируемых результатов освоения образовательной программы	3
1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы .	3
2. Место дисциплины (модуля) в структуре образовательной программы	3
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	3
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)	4
5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю).....	7
6. Учебно-методическое и информационное обеспечение дисциплины (модуля)	10
6.1. Перечень учебной литературы, необходимой для освоения дисциплины	10
6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем	11
6.3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства	14
7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)	15

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 понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)

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 понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)	1 этап: Знания	Обучающийся должен знать: основные принципы формирования и назначение информации в развитии современного общества
	2 этап: Умения	Обучающийся должен уметь: применять информационные технологии для поиска и обработки информации
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: навыками применения современных информационных технологий для поиска и обработки данных с учетом информационной безопасности

2. Место дисциплины (модуля) в структуре образовательной программы

В структуре образовательной программы дисциплина "Теоретические основы защиты информации" находится в базовой части

Дисциплина изучается на 2 курсе в 3 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 2 зач. ед., 72 акад. ч.

Объем дисциплины	Всего часов
	Очная форма обучения
Общая трудоемкость дисциплины	72
Учебных часов на контактную работу с преподавателем: лекций	16

практических (семинарских)	
лабораторных	16
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	
зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	39,8

Формы контроля	Семестры
зачет	3

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	8	0	8	20
1.1	Основные понятия теории информационной безопасности	2	0	2	5
1.2	Информация как объект защиты	2	0	2	5
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	2	0	2	5
1.4	Угрозы информационной безопасности	2	0	2	5
2	Модуль 2	8	0	8	19,8
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	2	0	2	5
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	2	0	2	5
2.3	Политика и модели безопасности	2	0	2	5
2.4	Обзор международных стандартов информационной безопасности	2	0	2	4,8
	Итого	16	0	16	39,8

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Модуль 1	
1.1	Основные понятия теории информационной безопасности	История становления и предметная область теории информационной безопасности. Систематизация

		<p>понятий в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации»</p> <p>Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации.</p>
1.2	Информация как объект защиты	<p>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</p>
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	<p>Информационная безопасность и ее место в системе национальной безопасности Российской Федерации. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность</p>
1.4	Угрозы информационной безопасности	<p>Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.</p>
2	Модуль 2	
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	<p>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.</p>
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	<p>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.</p>
2.3	Политика и модели безопасности	<p>Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения</p>

		<p>доступа</p> <p>Политика и модели мандатного доступа.</p> <p>Теоретико-информационные модели. Политика и модели тематического разграничения доступа.</p> <p>Ролевая модель безопасности.</p>
2.4	Обзор международных стандартов информационной безопасности	<p>Роль стандартов информационной безопасности.</p> <p>Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC).</p> <p>Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000.</p>

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Модуль 1	
1.1	Основные понятия теории информационной безопасности	<p>Систематизация понятий в области защиты информации. Основные термины и определения понятий в области информационной защиты информации. Принципы построения систем защиты. Задачи защиты информации.</p> <p>Средства реализации комплексной защиты информации</p>
1.2	Информация как объект защиты	<p>Уровни представления информации. Виды и формы представления информации. Свойства защищаемой информации. Структура и шкала ценности информации. Классификация информационных ресурсов.</p>
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	<p>Роль и место информационной безопасности в системе национальной безопасности РФ.</p> <p>Нормативная деятельность, функции и задачи органов обеспечения информационной безопасности и защиты информации.</p>
1.4	Угрозы информационной безопасности	<p>Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз.</p> <p>Неформальная модель нарушителя. Оценка уязвимости системы.</p>
2	Модуль 2	
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	<p>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.</p> <p>Защита от угрозы нарушения конфиденциальности информации.</p>

№ п/п	Тема и содержание	Задания по самостоятельной работе студентов
----------	-------------------	---

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.

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

		СР	
1	2	6	8
1.	Модуль 1.	20	
1.1.	Основные понятия теории информационной безопасности	5	подготовка к индивидуальному опросу;
1.2.	Информация как объект защиты	5	подготовка к индивидуальному опросу; подготовка к лабораторным работам; подготовка к контрольной работе;
1.3.	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	5	подготовка к индивидуальному опросу; подготовка к лабораторным работам; подготовка к контрольной работе;
1.4.	Угрозы информационной безопасности	5	подготовка к индивидуальному опросу; подготовка к лабораторным работам; подготовка к контрольной работе;
2.	Модуль 2.	19,8	
2.1.	Построение систем защиты от угрозы нарушения конфиденциальности	5	подготовка к индивидуальному опросу; подготовка к лабораторным работам;
2.2.	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	5	подготовка к индивидуальному опросу; подготовка к лабораторным работам;
2.3.	Политика и модели безопасности	5	подготовка к индивидуальному опросу; подготовка к лабораторным работам; подготовка к тестированию;
2.4.	Обзор международных стандартов информационной безопасности	4,8	подготовка к индивидуальному опросу; подготовка к лабораторным работам;
	Всего часов:	39,8	

Внеаудиторными формами и инструментами самостоятельной работы студентов по дисциплине являются: работа с конспектом лекций, изучение дополнительного теоретического материала, подготовка к занятиям, тестированию/контрольной работе и пр.

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.

Вопросы для самоконтроля

1. Чем отличаются понятия «информационная война» и «информационное противоборство»?
2. Чем отличается информационная война от обычного вооруженного конфликта?
3. Какие виды информационных войн Вы можете выделить?
4. Приведите пример межкорпоративной информационной войны.
5. Можно ли рассматривать рекламу как средство ведения информационной борьбы?
6. Какие приемы ведения информационной войны используются во время предвыборных кампаний, приведите примеры.
7. Что такое информационное оружие? Какие виды оружия применяются в ходе ведения информационной войны?
8. Каковы цели информационной войны?
9. Каковы средства и методы защиты от информационно-технического оружия?
10. Каковы особенности информационно-психологической войны?

Рекомендуемая учебно-методическая литература:

1. Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации): юридическая ответственность за правонарушения : учебное пособие / В. К. Новиков. – Москва : Горячая линия – Телеком, 2015. – 175 с. : ил., схем., табл. – Режим доступа: по подписке. –
URL: <https://biblioclub.ru/index.php?page=book&id=457171> (дата обращения: 20.06.2021).
2. Основы управления информационной безопасностью: учебное пособие для вузов / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва : Горячая

линия – Телеком, 2013. – 244 с. : ил. – (Вопросы управления информационной безопасностью. Вып. 1). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=253575> (дата обращения: 20.06.2021).

3. Беляков, С. Л. Основы разработки программ на языке C++ для систем информационной безопасности : учебное пособие : [16+] / С. Л. Беляков, А. В. Боженюк, М. В. Петряева ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – 152 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=612164> (дата обращения: 20.06.2021).

4. Сычев, Ю. Н. Основы информационной безопасности: учебно-практическое пособие : учебное пособие / Ю. Н. Сычев. – Москва : Евразийский открытый институт, 2010. – 328 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=90790> (дата обращения: 20.06.2021).

5. Галатенко, В. А. Основы информационной безопасности: Курс лекций : учебное пособие / В. А. Галатенко ; под ред. В. Б. Бетелина. – Изд. 3-е. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2006. – 208 с. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=233063> (дата обращения: 20.06.2021).

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

6.1. Перечень учебной литературы, необходимой для освоения дисциплины

Основная учебная литература:

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. 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).
3. Гультяева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гультяева. – 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).

Дополнительная учебная литература:

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. 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: 20.06.2021).

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 03.03.2023

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

№ п/п	Адрес (URL)	Описание страницы
1	http://www.securityportal.ru/	Сайт по защите информации, защите приватности, безопасным сетевым взаимодействиям, криптографии
2	http://www.oszone.net/6213/	Обеспечение безопасности детей при

		работе в Интернет (статья, ссылки, материалы)
3	http://www.anti-malware.ru/	Независимый информационно-аналитический портал по безопасности
4	http://www.securitylab.ru/software/1423/	Каталог программ «Защита детей от интернет угроз» (описание, сравнение, оценки)
5	http://internetsecure.ru/	Набор технологий и программ для безопасной работы в сети с компьютером
6	http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?id=cs_teach_kids	Вопросы безопасности — сайт от компании Symantec
7	http://www.citforum.ru/security/	CITFORUM — информационная безопасность (большое количество материалов по теме)
8	http://saferinternet.ru/	Портал Российского Оргкомитета по проведению Года Безопасного Интернета (ресурсы, ссылки, документы, материалы по

		проблематике)
9	http://www.infoforum.ru/	Национальный форум информационной безопасности "ИНФОФОРУМ" — электронное периодическое издание по вопросам информационной безопасности
10	http://ru.wikipedia.org/wiki/Netiquette	Сетевой этикет — Википедия
11	https://securelist.ru/enciklopediya	Энциклопедия информационной безопасности
12	http://laste.arvutikaitse.ee/rus/html/etusivu.htm	Основы безопасности в Интернете для молодежи интерактивный курс по Интернет-безопасности
13	http://www.content-filtering.ru/	Интернет-СМИ "Ваш личный Интернет" - помощь родителям в организации безопасного доступа детей в сеть Интернет
14	http://www.itn.ru/communities.aspx?cat_no=71586&tmpl=com	Обеспечение информационной безопасности в учебных заведениях. 4 этапа защиты компьютера — советы от компании

15	http://www.microsoft.com/rus/protect/default.mspx#	Microsoft. Вопросы обеспечения информационной безопасности от компании Microsoft
16	http://nicekit.ru/	Программа родительского контроля
17	http://download.live.com/familysafety	Семейная безопасность — Windows Live - программа от компании Microsoft
18	http://www.antispam.ru/	Проект Антиспам.Ру
19	http://www.etika.ru/	Этика — сайт создан специально для пользователей Рунета, которые хотят работать в этичной, корректной и безопасной среде и готовы участвовать в создании такой среды

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

Наименование программного обеспечения
AcademicEdition Networked Volume Licenses RAD Studio XE5 Professional Concurrent App / Плавающая – 60 шт. Бессрочная / ООО«Фермомобайл» / № 04182 от 03.12.2013
Kaspersky Endpoint Security / 950 / ООО «Смартлайн»/ №44/013 от 06.12.2021
Windows 10 Education N / Бессрочная / Microsoft Imagine. Подписка №8001361124 от 04.10.2017 г.
Office Standart 2010 RUS OLP NL Acdmс / 200, Бессрочная / ООО «Компания Фермо» / № Ф-04211 от 12.03.2021

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

Тип учебной аудитории	Оснащенность учебной аудитории
Читальный зал: помещение для самостоятельной работы	учебная мебель, учебно-наглядные пособия, компьютеры
Лаборатория информатики и вычислительной техники. 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, учебная аудитория курсового проектирования (выполнения курсовых работ).	Доска, проектор, экран, учебная мебель, компьютеры, учебно-наглядные пособия.
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.