

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 22.08.2025 10:48:49
Уникальный программный ключ:
b683afe664d7e9f64175886cf9626a196149ad36

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

Факультет Математики и информационных технологий
Кафедра Прикладной информатики и программирования

Рабочая программа дисциплины (модуля)

дисциплина **Техническая защита информации**

Блок Б1, базовая часть, Б1.Б.28

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., заведующий кафедрой
Хасанов М. К.
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	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.....	5
4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)	5
4.2. Содержание дисциплины, структурированное по разделам (темам)	5
5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю).....	7
6. Учебно-методическое и информационное обеспечение дисциплины (модуля)	8
6.1. Перечень учебной литературы, необходимой для освоения дисциплины	8
6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем	8
6.3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства	9
7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)	9

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 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 (ОПК-7)

Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)

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 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 (ОПК-7)	1 этап: Знания	Обучающийся должен знать: 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
	2 этап: Умения	Обучающийся должен уметь: 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
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: навыками определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)	1 этап: Знания	Обучающийся должен знать: особенности установки, настройки и обслуживания программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
	2 этап: Умения	Обучающийся должен уметь: выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: навыками выполнения работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

2. Место дисциплины (модуля) в структуре образовательной программы

Для освоения дисциплины студенты используют знания, умения и навыки, сформированные в процессе изучения дисциплин «Сети и системы передачи информации», «Администрирование информационных систем».

Цель освоения дисциплины настоящего курса является теоретическая и практическая подготовленность обучающегося к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в защищаемых помещениях

Дисциплина изучается на 3 курсе в 5, 6 семестрах

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 7 зач. ед., 252 акад. ч.

Объем дисциплины	Всего часов
	Очная форма обучения
Общая трудоемкость дисциплины	252

Учебных часов на контактную работу с преподавателем:	
лекций	28
практических (семинарских)	44
лабораторных	24
другие формы контактной работы (ФКР)	1,4
Учебных часов на контроль (включая часы подготовки):	34,8
зачет	
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	119,8

Формы контроля	Семестры
зачет	5
экзамен	6

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	12	0	40
1.1	Характеристика государственной системы противодействия технической разведке	4	6	0	20
1.2	Свойства и виды информации	4	6	0	20
2	Модуль 2	20	32	24	79,8
2.1	Демаскирующие признаки объектов наблюдения и сигналов	4	8	6	20
2.2	Средства и методы технической разведки	4	8	6	20
2.3	Способы и средства перехвата сигналов	6	8	6	20
2.4	Технические каналы утечки информации. Оптические, электромагнитные радиоэлектронные, акустические и виброакустические каналы утечки информации каналы утечки информации	6	8	6	19,8
	Итого	28	44	24	119,8

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Модуль 1	
1.1	Характеристика государственной системы противодействия	Нормативные документы по противодействию технической разведке

	технической разведке	
1.2	Свойства и виды информации	Виды, источники и носители защищаемой информации.
2	Модуль 2	
2.1	Демаскирующие признаки объектов наблюдения и сигналов	Опасные сигналы и их источники
2.2	Средства и методы технической разведки	Классификация технической разведки, основные этапы и процедуры добывания информации технической разведкой.
2.3	Способы и средства перехвата сигналов	Способы и средства наблюдения. Способы и средства подслушивания. Способы прослушивания помещений. Дистанционные системы прослушивания. Способы и средства добывания информации о радиоактивных веществах. Специальные системы получения информации
2.4	Технические каналы утечки информации. Оптические, электромагнитные радиоэлектронные, акустические и виброакустические каналы утечки информации каналы утечки информации	Технические каналы утечки информации. Оптические, электромагнитные радиоэлектронные, акустические и виброакустические каналы утечки информации каналы утечки информации

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Модуль 1	
1.1	Характеристика государственной системы противодействия технической разведке	Нормативные документы по противодействию технической разведке
1.2	Свойства и виды информации	Виды, источники и носители защищаемой информации.
2	Модуль 2	
2.1	Демаскирующие признаки объектов наблюдения и сигналов	Опасные сигналы и их источники
2.2	Средства и методы технической разведки	Классификация технической разведки, основные этапы и процедуры добывания информации технической разведкой.
2.3	Способы и средства перехвата сигналов	Способы и средства наблюдения. Способы и средства подслушивания. Способы прослушивания помещений. Дистанционные системы прослушивания. Способы и средства добывания информации о радиоактивных веществах. Специальные системы получения информации
2.4	Технические каналы утечки информации. Оптические, электромагнитные радиоэлектронные, акустические и виброакустические каналы утечки информации каналы утечки информации	Характеристики технических каналов утечки информации, физические принципы технических каналов передачи информации. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Электрические каналы утечки информации.

информации	информации. Материально-вещественные каналы утечки информации. Комплексное использование каналов утечки информации.
------------	--

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
2	Модуль 2	
2.1	Демаскирующие признаки объектов наблюдения и сигналов	Опасные сигналы и их источники
2.2	Средства и методы технической разведки	Классификация технической разведки, основные этапы и процедуры добывания информации технической разведкой.
2.3	Способы и средства перехвата сигналов	Способы и средства наблюдения. Способы и средства подслушивания. Способы прослушивания помещений. Дистанционные системы прослушивания. Способы и средства добывания информации о радиоактивных веществах. Специальные системы получения информации
2.4	Технические каналы утечки информации. Оптические, электромагнитные радиоэлектронные, акустические и виброакустические каналы утечки информации каналы утечки информации	Характеристики технических каналов утечки информации, физические принципы технических каналов передачи информации. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Электрические каналы утечки информации. Материально-вещественные каналы утечки информации. Комплексное использование каналов утечки информации.

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

Строгое соблюдение принципов постепенности и посильности и на всех этапах обучения является необходимым условием осмысленного усвоения материала.

Изучение дисциплины «Техническая защита информации» требует:

- прослушивания лекций преподавателя и дополнительное самостоятельное изучение разделов тем;
- выполнение лабораторных работ;
- выполнения индивидуальных, контрольных заданий и тестов;
- самостоятельную работу студентов.

Практические занятия предназначены для усвоения материала и включают:

- обсуждение наиболее значимых для дисциплины проблем, поиск связей с изученными ранее темами дисциплины «Техническая защита информации» и другими дисциплинами;
- подготовка ряда документов о проделанной работе;

- индивидуальные и групповые выступления.

Зачет - это проверка результатов теоретического и практического усвоения обучаемым учебного материала по дисциплине «Техническая защита информации».

Для студентов важна работа в диалоговом режиме контроля знаний и корректировка деятельности в процессе занятий и в последующей самостоятельной работе с материалом. Внеаудиторная самостоятельная работа студентов представляет собой вид занятий, которое каждый студент организует и планирует самостоятельно. Самостоятельная работа студентов включает:

- самостоятельное изучение разделов дисциплины;
- подготовку к практическим работам;

Прежде всего следует обратить внимание на изучение литературы и ресурсов Интернет, рекомендуемой преподавателем. Важно усвоение методических указаний. По каждой теме нужно изучить и запомнить перечень основных понятий. Задания тестов используются для самопроверки.

Если студент самостоятельно изучает дисциплину по индивидуальному графику, то форма контроля, сроки сдачи и основные вопросы для самостоятельной работы заранее необходимо обсуждать с преподавателем.

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

6.1. Перечень учебной литературы, необходимой для освоения дисциплины

Основная учебная литература:

1. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи : учебник : [16+] / Б. И. Филиппов, О. Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=499170>. – Библиогр.: с. 221-226. – ISBN 978-5-4475-9823-5. – DOI 10.23681/499170. – Текст : электронный
2. Прохорова, О. В. Информационная безопасность и защита информации : учебник : [16+] / О. В. Прохорова ; Самарский государственный архитектурно-строительный университет. – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=438331>. – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный

Дополнительная учебная литература:

1. Мельников, Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. – 2-е изд., стер. – Москва : ФЛИНТА, 2012. – 448 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=363419>. – Библиогр. в кн. – ISBN 978-5-9765-1613-7. – Текст : электронный

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	https://intuit.ru/	Бесплатное дистанционное обучение в Национальном Открытом Университете "ИНТУИТ"

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

Наименование программного обеспечения
Office Standart 2010 RUS OLP NL Acdmc / 200, Бессрочная / ООО «Компания Фермо» / № Ф-04211 от 12.03.2021
Windows 10 Education N / Бессрочная / Microsoft Imagine. Подписка №8001361124 от 04.10.2017 г.
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

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

Тип учебной аудитории	Оснащенность учебной аудитории
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
Лаборатория информатики и вычислительной техники. Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа,	Доска, проектор, экран, учебная мебель, компьютеры, учебно-наглядные пособия

<p>учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций, учебная аудитория курсового проектирования (выполнения курсовых работ)</p>	
<p>Лаборатория технической защиты информации. Помещение для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций</p>	<p>компьютеры; учебно-наглядные пособия; специализированное оборудование по защите информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок; технические средства контроля эффективности защиты информации от утечки по каналам</p>
<p>Читальный зал: помещение для самостоятельной работы</p>	<p>учебная мебель, учебно-наглядные пособия, компьютеры</p>