ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Утверждено
на заседании кафедры
протокол № 8 от «24» февраля 2021 г.
Зав. кафедрой _____ / Исмагилова А.С.

Согласовано
Председатель УМК института

_____ / Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информации в системах связи

Часть, формируемая участниками образовательных отношений

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль) подготовки
Организация и технологии защиты информации
(в системе государственного и
муниципального управления)

Квалификация
Бакалавр

Форма обучения
Очная

Разработчик (составитель)
Ассистент

_____ / Белова Е. П.

Для приема 2021 г.

Уфа - 2021 г.

Составитель: Белова Елена Петровна

Рабочая программа дисциплины утверждена на заседании кафедры управления информационной безопасностью, протокол № 8 от «24» февраля 2021 г.

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций
2. Цель и место дисциплины в структуре образовательной программы
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)
4. Фонд оценочных средств по дисциплине

   4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

   4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине.
5. Учебно-методическое и информационное обеспечение дисциплины

   5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

   5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

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

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
	ПК-4 - Способен выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях.	*ПК 4.1. Знать основные особенности функционирования программно-аппаратных средств защиты информации в компьютерных сетях.*	*Знает основные особенности функционирования программно-аппаратных средств защиты информации в компьютерных сетях.*
		ПК 4.2 Уметь управлять программно-аппаратными средствами защиты информации в компьютерных сетях.	*Умеет управлять программно-аппаратными средствами защиты информации в компьютерных сетях.*
		ПК 4.3 Владеть навыками анализа и выбора режимы работы программно-аппаратных средств защиты информации в компьютерных сетях.	*Владеет навыками анализа и выбора режимы работы программно-аппаратных средств защиты информации в компьютерных сетях.*

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Защита информации в системах связи» относится к части, формируемой участниками образовательных отношений.

Дисциплина изучается на 4 курсе в 1 семестре.

Целью учебной дисциплины «Защита информации в системах связи» является изучение методов и средств защиты информации в системах связи, а также получение навыков своевременного обнаружения уязвимостей.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

ПК-4 - Способен выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ПК 4.1 Знать основные особенности функционирования программно-аппаратных средств защиты информации в компьютерных сетях.	Знать основные особенности функционирования программно-аппаратных средств защиты информации в компьютерных сетях.	Не знает основные особенности функционирования программно-аппаратных средств защиты информации в компьютерных сетях.	Знает основные особенности функционирования программно-аппаратных средств защиты информации в компьютерных сетях.
ПК 4.2 Уметь управлять программно-аппаратными средствами защиты информации в компьютерных сетях.	Уметь управлять программно-аппаратными средствами защиты информации в компьютерных сетях.	Не умеет управлять программно-аппаратными средствами защиты информации в компьютерных сетях.	Умеет управлять программно-аппаратными средствами защиты информации в компьютерных сетях.
ПК 4.3 Владеть навыками анализа и выбора режимы работы программно-аппаратных средств защиты информации в компьютерных сетях.	Владеть навыками анализа и выбора режимы работы программно-аппаратных средств защиты информации в компьютерных сетях.	Не владеет навыками анализа и выбора режимы работы программно-аппаратных средств защиты информации в компьютерных сетях.	Владеет навыками анализа и выбора режимы работы программно-аппаратных средств защиты информации в компьютерных сетях.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей, перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).
Шкалы оценивания для зачета:

от 0 до 59 баллов – «не зачтено»;
от 60 до 100 баллов – «зачтено».

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Оценочные средства
ПК-4 - Способен выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях.	Знать основные особенности функционирования программно-аппаратных средств защиты информации в компьютерных сетях.	Аудиторная работа, тесты, устный опрос.
	Уметь управлять программно-аппаратными средствами защиты информации в компьютерных сетях.	Аудиторная работа, тесты, устный опрос.
	Владеть навыками анализа и выбора режимы работы программно-аппаратных средств защиты информации в компьютерных сетях.	Аудиторная работа, тесты, устный опрос.

Рейтинг-план
дисциплины «Защита информации в системах связи»

Виды учебной деятельности	**Балл за конкретное задание**	**Число заданий за семестр**	**Баллы**	
			Минимальный	**Максимальный**
Модуль 1. Микрофоны, антенны и средства перехвата информации				
Текущий контроль			**0**	35
1. Аудиторная работа	5	6	0	30
2. Устный опрос	1	5	0	5
Рубежный контроль			**0**	10
1.Тесты	1	10	0	10
Модуль 2. Противодействие средствам перехвата информации				
Текущий контроль			**0**	35
1. Аудиторная работа	5	6	0	30
2. Устный опрос	1	5	0	5
Рубежный контроль			**0**	10
1.Тесты	1	10	0	10
Поощрительные баллы				
1. Студенческая олимпиа-	5			5

да, участие в конференциях				
2. Публикация статей	5			5
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
Посещение лекционных занятий			0	–6
2. Посещение практических (семинарских, лабораторных занятий)			0	–10
Итоговый контроль				
Зачёт			0	0

Устный индивидуальный опрос

Устный индивидуальный опрос проводится после изучения новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации.

Обучающийся излагает содержание вопроса изученной темы.

Критерии и методика оценивания:

- 5 баллов выставляется обучающемуся, если точно используется специализированная терминология, показано уверенное владение нормативной базой;

- 4 балла выставляется обучающемуся, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология;

- 3 балла выставляется обучающемуся, нет общего понимания вопроса, имеются затруднения или допущены ошибки в определении понятий, использовании терминологии.

Устный групповой опрос

Устный групповой опрос проводится после изучения новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации, поддержания внимания слушающей аудитории.

Критерии и методика оценивания:

- 5 баллов выставляется обучающемуся, если точно используется специализированная терминология, показано уверенное владение нормативной базой;

- 4 балла выставляется обучающемуся, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология;

- 3 балла выставляется обучающемуся, нет общего понимания вопроса, имеются затруднения или допущены ошибки в определении понятий, использовании терминологии

Зачёт

Проводится в 7 семестре.

Типовые вопросы к зачёту:

1. Демаскирующие признаки сигналов.
2. Запись и съем информации с носителей.
3. Опасные сигналы и их источники.

4. Побочные преобразования акустических сигналов в электрические.
5. Паразитные связи и наводки.
6. Низкочастотные и высокочастотные излучения технических средств.
7. Электромагнитные излучения распределенных источников.
8. Утечка информации по системам электропитания и заземления.
9. Технические каналы утечки информации.
10. Акустические каналы утечки информации.
11. Оптические каналы утечки информации.
12. Радиоэлектронные каналы утечки информации.
13. Методы и средства защиты информации от ее утечки по техническим каналам.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей, перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).
Шкалы оценивания для зачета:
от 0 до 59 баллов – «не зачтено»;
от 60 до 100 баллов – «зачтено».

Тестирование. Примеры вопросов:

1. К принципам обеспечения безопасности относится:
а) согласованность;
б) взаимная ответственность личности, общества и государства;
в) децентрализации и демократизм.
2. Совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства:
а) угроза информационной безопасности;
б) предполагаемые действия иностранных государств;
в) деятельность иностранных разведок.
3. Не являются видами угроз информационной безопасности:
а) внутренние угрозы;
б) внешние угрозы;
в) значительные угрозы.
4. Не являются видами угроз информационной безопасности:
а) угрозы военные;
б) угрозы потенциальные;
в) угрозы реальные.
5. К методам обеспечения информационной безопасности Российской Федерации относятся:
а) правовые;
б) неправовые;
в) легальные.
6. К методам обеспечения информационной безопасности Российской Федерации относятся:
а) методы принуждения;
б) организационно-технические;
в) секретные.
7. К методам обеспечения информационной безопасности Российской Федерации относятся:
а) оперативные;

б) конструктивные;

в) экономические.

8. Сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации это:

а) сфера хранения информации;

б) информационная сфера;

в) сфера государственного регулирования информации.

Критерии оценивания теста

В комплекте тестов 25 вопросов,

за один правильный ответ ставится 0.4 балла.

За тест максимальный балл 10 баллов .

Творческое задание (презентация, доклад)

Выполняется по результатам изучения темы дисциплины с целью дополнения практического материала.

Примеры тем творческих заданий:

1. Законодательная база в области защиты информации.
2. Структура государственных органов обеспечивающих защиту информации.
3. Общая характеристика организационных методов ЗИ.
4. Общие критерии безопасности информации.
5. Действующие стандарты РФ по защите информации.
6. Понятие политики безопасности.
7. Уязвимости. Модели основных политик от НСД.
8. Особенности защиты информации в системах связи.
9. Криптография.
10. Стеганография.
11. Защита компьютерных сетей.

Критерии и методика оценивания:

Подготовленная и оформленная в соответствии с требованиями работа (презентация, доклад) оценивается преподавателем по следующим критериям:

- уровень эрудированности автора по изученной теме (знание автором состояния изучаемой проблематики, цитирование источников, в т.ч. НПА);
- логичность подачи материала, грамотность автора;
- соответствие работы всем стандартным требованиям к оформлению;
- знания и умения на уровне требований стандарта данной дисциплины: знание фактического материала, усвоение общих понятий и идей.
- 0 баллов выставляется студенту, если работа не соответствует критериям;
- 1 балл выставляется студенту, если работа частично соответствует критериям;
- 3 балла выставляется студенту, если работа соответствует критериям, но отсутствует логичность изложения информации;

– 5 баллов выставляется студенту, если работа полностью соответствует критериям.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - Москва : Горячая линия-Телеком, 2015. - 585 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0424-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457143

2. Малюк, А.А. Защита информации в информационном обществе : учебное пособие / А.А. Малюк. - Москва : Горячая линия-Телеком, 2015. - 229 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0481-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457170

3. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности : учебное пособие / Ю.И. Коваленко. - Москва : Горячая линия - Телеком, 2012. - 140 с. : ил. - Библиогр. в кн. - ISBN 978-5- 9912-0261-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253538

Дополнительная литература:

1. Аверченков, В.И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5- 9765-1271-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356

2. Семь безопасных информационных технологий [Электронный ресурс] : учебник / А.В. Барабанов [и др.] ; под ред. Маркова А.С.. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 224 с. — Режим доступа: https://e.lanbook.com/book/97352. — Загл. с экрана.

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
2. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
3. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
4. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
5. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
6. www.newlibrary.ru – Новая электронная библиотека;
7. www. edu.ru – Федеральный портал российского образования;
8. www.elibrary.ru – Научная электронная библиотека;
9. www.nehudlit.ru – Электронная библиотека учебных материалов.
10. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
11. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
12. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специальных помещений и помещений для самостоятельной работы	*Вид занятий*	*Наименование оборудования, программного обеспечения*
1	**2**	**3**
Аудитория № 516	Лекции, семинары, практические занятия.	Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование.
Аудитория № 610	Лекции, семинары, практические занятия.	Учебная мебель, доска, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м.
Аудитория № 609	Лекции, семинары, практические занятия.	Учебная мебель, доска, мобильное мультимедийное оборудование.
Аудитория № 608	Лекции, семинары, практические занятия.	Учебная мебель, доска, мобильное мультимедийное оборудование
Аудитория № 613	Практические занятия, лабораторные работы.	Учебная мебель, доска, моноблок стационарный – 12 шт. с возможностью подключения к сети Интернет и доступа в электронную информационно-образовательную среду. Windows 8 Russian Windows Professional 8 Russian Upgrade. Договор №104 от 17.06.2013 г. Лицензии бессрочные. Microsoft Office Standard 2013 Russian. Договор №114 от 12.11.2014 г. Лицензии бессрочные.

Приложение 1

МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Содержание рабочей программы
дисциплины «Защита информации в системах связи»
на 7 семестр ОФО

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 ЗЕТ / 72 часа
Учебных часов на контактную работу с преподавателем:	36,2
лекций	8
практических/ семинарских	28
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0
Учебных часов на самостоятельную работу обучающихся (СР)	20

Форма контроля:
зачёт 7 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛР	СР		
1	2	3	4	5	6	7	8
1.	**Модуль 1. Микрофоны, антенны и средства перехвата информации** **Раздел 1. Микрофоны и антенны:** 1.1. Микрофоны. 1.2. Акустические антенны. 1.3. Выбор типа микрофона и места его установки. **Раздел 2.** **2.1. Средства перехвата информации:** 2.2. Изучение устройств для перехвата речевой информации в проводных каналах. 2.3. Изучение оптико-акустической аппаратуры перехвата речевой информации. 2.4. Оптико-	4	6	8	10	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Аудиторная работа, тесты

	механические приборы. 2.5. Приборы ночного видения. 2.6. Средства скрытой фотосъемки. 2.7. Зоны подключения в линиях связи. 2.8. Перехват телефонных переговоров в зонах «А», «Б», «В», «Г», «Д», «Е». 2.9. Панорамные приемники.						
2.	**Модуль 2. Раздел 3: Противодействие средствам перехвата информации** **Раздел 3: Противодействие средствам перехвата информации:** 3.1. Изучение средств перехвата информации. 3.2. Изучение устройств подавления микрофонов. 3.3. Изучение перехвата сообщений в каналах сотовой связи. 3.4. Методы поиска закладных устройств	4	6	8	10	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Аудиторная работа, тесты

	как физических объектов и электронных средств. 3.5. Аппаратура контроля и защиты линии связи. 3.6. Средства создания акустических и электромагнитных маскирующих помех.						
	Всего часов	8	12	16	20		