Образовательное учреждение профсоюзов
высшего образования
«АКАДЕМИЯ ТРУДА И СОЦИАЛЬНЫХ ОТНОШЕНИЙ»

БАШКИРСКИЙ ИНСТИТУТ СОЦИАЛЬНЫХ ТЕХНОЛОГИЙ (филиал)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.15.06 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки
09.03.03 Прикладная информатика
(код и наименование направления подготовки)

Профиль (программа) подготовки
Прикладная информатика
(направленность (профиль) (уровень бакалавриата)

Квалификация выпускника
Бакалавр

2023

1. **Целью дисциплины** является:
   - развитие компетенций:

ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Индикаторы достижения:

Знание основ информационной и библиографической культуры (ОПК-3.1).

Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий (ОПК-3.2).

Показывать навыки работы с базами данных с учетом основных требований информационной безопасности (ОПК-3.3).

2. **Трудоемкость учебной дисциплины** зафиксирована учебным планом соответствующей основной профессиональной образовательной программы, выражается в зачетных единицах. Одна зачетная единица равна 36 академическим часам продолжительностью 45 минут (27 астрономическим часам по 60 минут) и включает часы контактной работы и часы самостоятельной работы студента, в том числе часы, отводимые на процедуры контроля и подготовку к ним.

3. **Результаты освоения образовательной программы:**

В результате изучения дисциплины обучающийся должен:

Знать:

– нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий;

– сущность и значение информации в развитии современного информационного общества;

– основы организации ИТ-инфраструктуры и управлении информационной безопасностью;

Уметь:

– использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий;

– разбираться в сущности и значении информации в развитии современного информационного общества, сознавая опасности и угрозы, возникающие в этом процессе;

– принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью;

Владеть:

– способность использования нормативно-правовых документов, международных и отечественных стандартов в области информационных систем и технологий;

– способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

– способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью.

4. Место дисциплины (модуля) в структуре образовательной программы:

Дисциплина «Информационная безопасность» относится к базовой части учебного плана.

5. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание раздела
1.	**Раздел 1. Понятие информационной безопасности.**	Основные составляющие информационной безопасности. Актуальность проблемы. Понятие информационной безопасности. Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности.
2.	**Раздел 2. Распространение объектно-ориентированного подхода на информационную безопасность.**	О необходимости объектно-ориентированного подхода к информационной безопасности. Основные понятия объектно-ориентированного подхода. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения.
3.	**Раздел 3. Виды угроз и законодательство по информационной безопасности.**	**Тема 3.1. Наиболее распространенные угрозы.** Основные определения и критерии классификации угроз. Наиболее распространенные угрозы доступности. Некоторые примеры угроз доступности. Вредоносное программное обеспечение. Основные угрозы целостности. Основные угрозы конфиденциальности. **Тема 3.2. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности.** Законодательство Российской Федерации в области информационной безопасности. Информация как объект юридической и физической защиты. Государственные информационные ресурсы. Защита государственной тайны как особого вида защищаемой информации. Защита конфиденциальной информации, в том числе интеллектуальной собственности и коммерческой тайны. Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа. Компьютерные преступления и особенности их расследования. Оценочные стандарты и технические спецификации. "Оранжевая

		книга" как оценочный стандарт.
4.	**Раздел 4. Основы кодирования, шифрования и встраивания скрытой информации.**	**Тема 4.1. Криптографические методы.** Основные понятия и определения. Понятие криптографического протокола. Основные типы протоколов. Классы преобразований: подстановки, перестановки, гаммирование, блочные шифры. Датчики ПСЧ. Симметричная криптография. Асимметричная криптография. Цифровой дайджест и хэш-функция. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома, Хилла. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома. **Тема 4.2. Симметричные и асимметричные криптографические системы.** Стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. Стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования. Блочные алгоритмы. Алгоритм Blowfish. Потоковые алгоритмы. Алгоритм PKZIP. Теоретическая и практическая стойкость. Системы с открытым ключом. Алгоритм шифрования RSA. Вычислительные аспекты реализации алгоритма RSA. Вопросы стойкости. **Тема 4.3. Электронная цифровая подпись.** Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Алгоритм безопасного хэширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции. Электронная подпись на основе алгоритма RSA. Алгоритм цифровой подписи Эль-Гамаля (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи. Тема 4.4. Методы и средства встраивания скрытой служебной информации. Понятие стеганографии. Задача встраивания скрытой служебной информации (цифровых водяных знаков) в аудио и видеосигналы для управления правами доступа к информационным ресурсам. Основные методы и алгоритмы встраивания и обнаружения водяных знаков. Встраивание водяных знаков и сжатие информации. Виды атак на информационные ресурсы, содержащие водяные знаки.
5.	**Раздел 5. Основы безопасности сетевых технологий.**	**Тема 5.1. Безопасность современных сетевых технологий.** Способы несанкционированного доступа к информации в компьютерных сетях. Классификация способов несанкционированного доступа и жизненный цикл атак. Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Особенности межсетевого экранирования на различных уровнях модели OSI. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Критерии оценки межсетевых экранов. Построение защищенных виртуальных сетей. Способы создания защищенных

		виртуальных каналов. Обзор протоколов. **Тема 5.2. Безопасность в открытых сетях.** Инфраструктура на основе криптографии с открытыми ключами (ИОК). Цифровые сертификаты. Управление цифровыми сертификатами. Компоненты ИОК и их функции. Центр Сертификации. Центр Регистрации. Конечные пользователи. Сетевой справочник. Использование ИОК в приложениях. Электронная почта и документооборот. Web приложения.

Рекомендуемая тематика учебных занятий в форме контактной работы:
Рекомендуемая тематика учебных занятий лекционного типа (предусматривающих преимущественную передачу учебной информации преподавателями):
Тема 3.1. Наиболее распространенные угрозы
Тема 3.2. Законодательный уровень информационной безопасности.
Стандарты и спецификации в области информационной безопасности
Тема 4.1. Криптографические методы
Тема 4.2. Симметричные и асимметричные криптографические системы
Тема 4.3. Электронная цифровая подпись
Тема 5.1. Безопасность современных сетевых технологий
Тема 5.2. Безопасность в открытых сетях

Рекомендуемая тематика учебных занятий семинарского типа (семинары, практические занятия, коллоквиумы и иные аналогичные занятия)
Тема 1: **Понятие информационной безопасности.**
Вопросы для обсуждения:
1. Составляющие информационной безопасности
2. Проблемы информационной безопасности
3. Актуальность проблемы информационной безопасности
4. Методы информационной безопасности
5. Информационная безопасность на предприятии
Тема 2: **Распространение объектно-ориентированного подхода на информационную безопасность.**
Вопросы для обсуждения:
1. Объектно-ориентированного подход в решении проблем информационной безопасности
2. Основные понятия объектно-ориентированного подхода
3. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем
4. Недостатки традиционного подхода к информационной безопасности
5. Подходы к решению проблем информационной безопасности на современном этапе

Тема 3: **Виды угроз и законодательство по информационной безопасности.**

Вопросы для обсуждения:

1. Определение угрозы информационной безопасности
2. Угрозы доступности
3. Законодательство Российской Федерации в области информационной безопасности
4. Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа.
5. Компьютерные преступления

Тема 4: **Криптографические методы.**

Вопросы для обсуждения:

1. Криптография
2. Симметричная и асимметричная криптография
3. Разновидности шифров
4. Стандарт шифрования DES
5. Алгоритм PKZIP

Тема 5: **Основы безопасности сетевых технологий.**

Вопросы для обсуждения:

1. Способы несанкционированного доступа к информации в компьютерных сетях
2. Особенности межсетевого экранирования на различных уровнях модели OSI
3. Режим функционирования межсетевых экранов и их основные компоненты
4. Критерии оценки межсетевых экранов
5. Безопасность в открытых сетях

Требования к самостоятельной работе студентов по освоению дисциплины

Самостоятельная работа студентов при изучении дисциплины «Информационная безопасность» направлена на решение следующих задач:

изучение программно-аппаратных средств защиты информации, методов анализа и планирования информационной защиты компьютерных систем, сетей и их компонентов, средств защиты сетевых служб.

Результаты самостоятельной работы контролируются преподавателем и учитываются при текущей аттестации студента. При этом проводятся: тестирование, экспресс-опрос на практических занятиях, заслушивание докладов, проверка письменных работ и т.д. Несомненно, умение анализировать юридические источники, работать с литературой, навыки поиска, обработки и оформления необходимой информации, способность обосновывать собственную позицию помогут студенту в дальнейшей самостоятельной учебной и научной работе.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно

выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).
Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

Примерная тематика рефератов для самостоятельных работ

1. Роль защиты информации в обществе.
2. Составляющие информационной безопасности.
3. Парольная защита информации.
4. Классификация вредоносного ПО.
5. Информационная безопасность в организации.
6. Методы кодирования и декодирования информации.
7. Электронная цифровая подпись.
8. Блочные алгоритмы.
9. Встраивание скрытой служебной информации.
10. Криптография.
11. Несанкционированный доступ в компьютерных сетях.
12. Методы противодействия несанкционированному доступу.
13. Криптография с открытыми ключами.
14. Межсетевые экраны.
15. Виртуальные защищенные сети.
16. Политика информационной безопасности в РФ.
17. Виды угоз информационной безопасности.
18. Системы управления информационной безопасностью.
19. Объектно-ориентированный подход в системах безопасности.
20. Системный подход в информационной безопасности.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ "Об образовании в Российской Федерации" научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы,

пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

6. **Виды учебной работы по дисциплине** зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах.

Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения.

Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно- образовательной среды института с использованием ресурсов сети Интернет и дистанционных технологий.

7. Учебно-методическое обеспечение дисциплины:

основная литература:

1. Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие : [16+] / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова. – Москва : Директ-Медиа, 2022. – 128 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=694670 – Библиогр.: с. 117-118. – ISBN 978-5-4499-3327-0. – Текст : электронный.

2. Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.

3. Преступления в сфере высоких технологий и информационной безопасности : учебное пособие : [16+] / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина ; под науч. ред. А. Г. Волеводза ; Московский государственный институт международных отношений (Университет) Министерства иностранных дел Российской Федерации. – Москва : Прометей, 2023. – 1086 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=701090 – Библиогр. в кн. – ISBN 978-5-00172-447-6. – Текст : электронный.

дополнительная литература:

1. Мельников, В.П. Информационная безопасность и защита информации [Текст] : учебное пособие для студентов высших учебных заведений / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - 3-е изд., стер. - М. : Academia, 2008. - 336 с. - (Высшее профессиональное образование : информатика и вычислительная техника).

2. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576726 – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный.

8. Перечень программного обеспечения, информационных справочных систем и интернет - ресурсов, необходимых для освоения дисциплины

Операционная системаWindows XP Professional Service Pack 3: инв. №931, 932, 934, 936, 938, 940, 941, 942, 953: (Договор б\н от 29.03.2008) инв. №21747-217450, 21798, 21808: Лицензии № 42302228
Microsoft Office Professional Plus 2007 Лицензии № 42302228
Star Board Software (Договор Б/Н от 20.11.2008)
Антивирус: Kaspersky Endpoint Security 10 (Договор № 5337-ПАО/2015 от 30.09.2015 г.)
Доступ в интернет: Договор № RK 10091-08 от 31.12.2013
Справочная правовая система Консультант Плюс (Договор №3/4 от 01.02.2012 г.)

9. Требования к материально-техническому и учебно-методическому обеспечению дисциплины:

Для проведения занятий лекционного типа используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой.

Лекционные и практические занятия проводятся в аудиториях, оснащенных презентационным оборудованием (компьютер, имеющий выход в Интернет, мультимедийный проектор, экран, акустические системы), доской, рабочими учебными столами и стульями.

При необходимости занятия проводятся в компьютерных классах, оснащенных доской, экраном, рабочими учебными столами и стульями, персональными компьютерами, объединенными в локальные сети с выходом в Интернет, с установленным лицензионным программным обеспечением, с подключенным к ним периферийным устройством и оборудованием (мультимедийный проектор, акустическая система и пр.).

Для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), консультаций, текущего контроля и промежуточной аттестации достаточно специальных помещений (учебных аудиторий), оборудованных специализированной мебелью (для обучающихся) меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду института.

– **Образовательные технологии**

В процессе освоения дисциплины используются следующие образовательные технологии:

1. **Стандартные методы обучения:**

– лекции;
– практические занятия, на которых обсуждаются основные проблемы, освещенные в лекциях и сформулированные в домашних заданиях;
– письменные или устные домашние задания;
– самостоятельная работа студентов, в которую входит освоение теоретического материала, подготовка к практическим занятиям, выполнение указанных выше письменных/устных заданий, работа с литературой.

2. **Методы обучения с применением интерактивных форм образовательных технологий:**

– интерактивные лекции;
– компьютерные симуляции;
– анализ деловых ситуаций на основе кейс-метода и имитационных моделей;
– деловые и ролевые игры;
– круглые столы;
– групповые дискуссии и проекты

– **Требования к промежуточной аттестации и оценочные материалы для ее проведения**

Промежуточная аттестация выполняется в форме экзамена.

Оценочные материалы текущего контроля и промежуточной аттестации представлены в форме вопросов для зачета с оценкой. Примерные вопросы, задания, темы рефератов для проведения промежуточной аттестации по дисциплине и критерии оценивания представлены на сайте (https://ufabist.ru/sveden/education/eduop/)

В полном объеме оценочные материалы хранятся на кафедре, реализующей данную дисциплину.

Разработчик:
К.т.н., доцент кафедры экономики и информационных технологий
А.И. Быстров