ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

«УТВЕРЖДАЮ»
Директор института математики, естествознания и техники
_____ /Н.В.Черноусова/

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
# ФТД.В.02 Безопасность информационных систем и технологий

**Направление подготовки:** 09.04.01 Информатика и вычислительная техника
**Направленность (профиль):** Автоматизированные системы обработки информации и управления
**Квалификация (степень):** *магистр*
**Форма обучения:** *очная*
**Институт:** математики, естествознания и техники
**Кафедра:** математического моделирования, компьютерных технологий и информационной безопасности

| | **очная форма** | **очно-заочная форма** | **заочная форма** |
|---|---|---|---|
| **Курс** | **1** | | |
| **Семестр/триместр** | **2** | | |
| | | | |
| **Лекции** | **18** | | |
| **Лабораторные занятия** | **-** | | |
| **Практические (семинарские) занятия** | **-** | | |
| **Консультации** | **-** | | |
| **Форма(ы) промежуточной аттестации** | **Зачет во 2 семестре** | | |
| **Контроль** | **-** | | |
| **Иные формы работы** | - | | |
| **Самостоятельная работа** | **18** | | |

**Всего часов: 36**
**Трудоемкость: ___1__ зачетная единица.**
Разработчик(и) рабочей программы:
кандидат физико-математических наук, доцент кафедры ММКТиИБ Рощупкин С.А.

# I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

**Цель изучения дисциплины:**

Цель изучения дисциплины ФТД.В.02 Безопасность информационных систем и технологий – формирование у студентов-магистрантов теоретических и прикладных компетенций в области организации и поддержания безопасности информационных систем и технологий.

**Задачи изучения дисциплины:**

– ознакомить с теоретическими, практическими и методическими вопросами классификации угроз информационных систем;
– ознакомить с основными способами организации и обеспечения безопасности информационных систем и технологий.

**Место дисциплины в структуре ОПОП:** реализуется в рамках вариативной части (части, формируемой участниками образовательных отношений) блока ФТД.Факультативные дисциплины (модули).

**Планируемые результаты обучения по дисциплине:**

| Код компетенции | Индикаторы достижения компетенции | Планируемые результаты обучения по дисциплине |
|---|---|---|
| **ПКС-1** | Знать:<br>– инструменты и методы согласования требований к информационной системе управления;<br>– современные подходы и стандарты автоматизации организации;<br>– предметную область автоматизации;<br>– инструменты и методы проектирования структур баз данных, информационных систем управления и их дизайна;<br>– регламенты развертывания информационных систем управления. | Знает:<br>– методы и приемы разработки информационно-коммуникационного обеспечения ИС;<br>– методы и приемы формализации задач;<br>– методы и средства проектирования информационно-коммуникационного обеспечения на основе средств компьютерного моделирования; |
| | Уметь:<br>– распределять работы и выделять ресурсы в рамках управления работами по сопровождению и проектами создания (модификации) информационных систем;<br>– управлять содержанием проекта: документирование | Умеет:<br>– использовать существующие типовые решения проектирования информационно-коммуникационного обеспечения ИС;<br>– выбирать средства реализации требований к базам данных ИС;<br>– вырабатывать варианты реализации баз данных ИС и требований к нему;<br>– проводить анализ исполнения требований; |

| | | |
|---|---|---|
| | требований, анализ продукта, модерируемые совещания;<br>– применять методики описания и моделирования бизнес-процессов, средства моделирования бизнес-процессов. | – ориентироваться в современных технических средствах реализации ИС. |
| | Владеть:<br>– организацией согласования и утверждения требований к информационной системе заказчиком в рамках управления работами по сопровождению и проектами создания (модификации) информационных систем;<br>– обеспечением соответствия проектирования и дизайна информационных систем, принятым в организации или проекте стандартам и технологиям в рамках управления работами по сопровождению и проектами создания (модификации) информационных систем;<br>– контролем исполнения в рамках управления работами по сопровождению и проектами создания (модификации) информационных систем;<br>– инструментами и методами оптимизации информационных систем управления. | Владеет:<br>– методологией организации процесса разработки информационно-коммуникационного обеспечения ИС;<br>– методологией и технологиями проектирования программных интерфейсов, структур и баз данных ИС в соответствии с установленными требованиями;<br>– действиями по разработке и согласованию технических спецификаций на программные компоненты;<br>– действиями по согласованию требований к базам данных ИС с заинтересованными сторонами, распределению заданий между программистами в соответствии с техническими спецификациями, осуществлению контроля выполнения заданий, формированию отчетности в соответствии с установленными регламентами. |

# II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

**с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу**

## Очная форма обучения

| № п/п | Наименование разделов и тем | Всего | Аудиторные занятия | | | Сам.раб. |
|---|---|---|---|---|---|---|
| | | | ЛК | ПЗ | ЛБ | |
| | **Раздел 1.** Обзор стандартов информационных систем | **8** | **4** | | | **4** |
| 1. | Тема 1. Особенности анализа и управления безопасностью информационных систем. | 4 | 2 | | | 2 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | Тема 2. Классификация стандартов по безопасности. Серия ISO/IEC 27000. Менеджмент информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США. Классы защищенности компьютерных систем | 4 | 2 | | | 2 |
| | **Раздел 2. Уязвимости информационных систем** | **8** | **4** | | | **4** |
| 3. | Тема 3. Анализ угроз ИБ ресурсам информационной системы и причины их реализации. | 4 | 2 | | | 2 |
| 4. | Тема 4. Слабости современных технологий программирования. Ошибки в программном обеспечении. Сетевые вирусы. | 4 | 2 | | | 2 |
| | **Раздел 3. Атаки на информационные системы.** | **8** | **4** | | | **4** |
| 5. | Тема 5. Удаленные атаки на информационные системы. Типичные сценарии и уровни атак. | 4 | 2 | | | 2 |
| 6. | Тема 6. Классические и современные методы, используемые нападающими для проникновения в информационные системы. | 4 | 2 | | | 2 |
| | **Раздел 4. Обеспечение информационной безопасности в информационных системах.** | **12** | **6** | | | **6** |
| 7. | Тема 7. Создания защищенных средств связи объектов в открытых системах на основе стандартов ISO 7498-2, 17799, 15408. Разработка политики безопасности для информационных систем. | 4 | 2 | | | 2 |
| 8. | Тема 8. Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление. | 4 | 2 | | | 2 |
| 9. | Тема 9. Средства обеспечения информационной безопасности в информационных системах. Создание комплексной системы обеспечения безопасности информационных систем. | 4 | 2 | | | 2 |
| | *Зачет* | | | | | |
| | *Итого за 2 семестр* | *36* | 18 | | | 18 |
| | в т.ч. практическая подготовка | | | | | |
| | ИТОГО: | 36 | 18 | | | 18 |

**Очно-заочная форма обучения *не реализуется.***

**Заочная форма *не реализуется.***

## III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

### Текущий контроль

Текущий контроль успеваемости, т.е. проверка усвоения учебного материала, регулярно осуществляемая на протяжении семестра. Текущий контроль знаний учащихся организован как устный групповой опрос.

Текущая самостоятельная работа студента направлена на углубление и закрепление знаний, и развитие практических умений студента.

Промежуточная аттестация обучающихся осуществляется в форме зачета с использованием следующих оценочных материалов:

### Вопросы к зачету
### (2 семестр, очная форма обучения)

1. Опишите средства защиты используемые в информационных системах.
2. Сетевые вирусы. Удаленные атаки на распределенные системы.
3. Типичные сценарии и уровни атак.
4. Классические и современные методы, используемые нападающими для проникновения в открытые системы.
5. Специфика защиты ресурсов распределенных систем на примере интранета.
6. Принципы создания защищенных средств связи объектов в распределенных системах.
7. Средства обеспечения информационной безопасности в распределенных системах.
8. Управление безопасностью распределенных систем.
9. Организационно-правовые методы защиты распределенных систем.
10. Аутентификация субъектов и объектов взаимодействия в распределенных системах.
11. Системы анализа защищенности.
12. Системы обнаружения и предотвращения вторжений.
13. Политика безопасности для информационных систем.
14. Создание комплексной системы обеспечения безопасности для информационных систем.

## IV.ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

### 4.1. Основная литература

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515435 .
2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998.

### 4.2. Дополнительная литература

1. Аверченков, В. И. Аудит информационной безопасности : учебное пособие / В. И. Аверченков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 269 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93245 – Библиогр. в кн. – ISBN 978-5-9765-1256-6. – Текст : электронный.

## V.ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

| № пп | Ссылка на информационный ресурс | Наименование разработки в электронной форме | Доступность |
|---|---|---|---|
| 1. | https://infourok.ru/ | **Инфоурок:** образовательный интернет-проект России. Включает: конспекты уроков, презентации, тесты, видеоуроки и другие материалы по предметам школьной программы. | Свободный доступ |
| 2. | http://edu.ru/ | **Российское образование: Федеральный портал. Включает** ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ. | Свободный доступ |
| 3. | www.intuit.ru/studies/courses | Информатика [Электронный ресурс] : открытые интернет-курсы «Интуит» //национальный открытый университет «Интуит» | Свободный доступ |

## VI.СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕСПРАВОЧНЫЕ СИСТЕМЫ

| № пп | Ссылка на информационный ресурс | Наименование разработки в электронной форме | Доступность |
|---|---|---|---|
| 1. | http://www.biblioclub.ru | Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн | Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет |
| 2. | www.elibrary.ru | Российский информационный портал в области науки, технологии, медицины и образования | Свободный доступ |
| 3. | https://urait.ru/ | Образовательная платформа Юрайт — образовательный ресурс, электронная библиотека и интернет-магазин, где читают и покупают электронные и печатные учебники авторов — преподавателей ведущих университетов для всех уровней профессионального образования, а также пользуются видео- и аудиоматериалами, тестированием и сервисами для преподавателей, доступными 24 часа 7 дней в неделю. | Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет |

## VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:
- Microsoft Windows;
- LibreOffice;
- Google Chrome / Mozilla Firefox
- VirtualBox

## VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.