

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное автономное образовательное учреждение  
высшего образования  
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ  
Директор по образовательной  
деятельности

*М.М.М.*



## РАБОЧАЯ ПРОГРАММА МОДУЛЯ

**Код модуля**  
*1156864*

**Модуль**  
*Основы информационной безопасности*

Екатеринбург, 2021

| Перечень сведений о рабочей программе модуля  | Учетные данные   |
|---|--|
| Образовательная программа<br><i>Информационная безопасность телекоммуникационных систем</i> | Код ОП 10.05.02/22.01                                  |
| Направление подготовки Информационная безопасность  | Код направления и уровня подготовки<br><i>10.05.02</i> |

Области образования, в рамках которых реализуется модуль образовательной программы по ФГОС ВО 3++ *специалитет*

| № п/п | Перечень областей образования, для которых разработан ФГОС ВО 3++ | Уровень подготовки |
|-------|---|--------------------|
| 1.    | Инженерное дело, технологии и технические науки                   | <i>специалитет</i> |

Программа модуля составлена авторами:

| № п/п | Фамилия Имя Отчество        | Ученая степень, ученое звание | Должность             | Подразделение   |
|-------|-----------------------------|-------------------------------|-----------------------|---|
| 1     | Поршнев Сергей Владимирович | д.т.н., профессор             | Директор УНЦ ИБ       | <i>Учебно-научный центр «Информационная безопасность»</i> |
| 2     | Пономарева Ольга Алексеевна |                               | Старший преподаватель | <i>Учебно-научный центр «Информационная безопасность»</i> |

**Руководитель модуля - С.В. Поршнев**

**Согласовано:**

Управление образовательных программ

Р.Х.Токарева

## ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Основы информационнор безопасности

### 1.1. Аннотация содержания модуля

Модуль «**Основы информационнор безопасности**» направлен на изучение вопросов обеспечения безопасности систем и каналов связи, режимных объектов, выделенных помещений и хранилищ, формирование качеств, необходимых для понимания, распознавания и реагирования на разнообразные умышленные угрозы, характерные для компьютерной преступности. Изучаются физические основы образования утечки информации по техническим каналам, принципы и устройства технической разведки. Противодействие опасному человеческому фактору реализуется в виде взаимосвязанного набора активных и пассивных действий.

### 1.2. Структура и объем модуля

Таблица 1

| № п/п | Перечень дисциплин модуля в последовательности их освоения | Объем дисциплин модуля и всего модуля в зачетных единицах и часах |
|-------|--|---|
| 1.    | (ББ) Основы информационной безопасности                    | 3/108   |
|       | ИТОГО по модулю:   | 3/108   |

### 1.3. Последовательность освоения модуля в образовательной программе

|                                     |   |
|-------------------------------------|---|
| Пререквизиты модуля                 |   |
| Постреквизиты и корреквизиты модуля | (ББ) Основы информационной безопасности |

### 1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Изучение дисциплин модуля предусматривает формирование компетенций посредством последовательного освоения результатов обучения на определенном уровне сложности содержания.

Результаты обучения по дисциплине – это конкретные знания, умения, опыт и другие результаты (содержательные компоненты компетенций), которых планируется достичь на этапе изучения дисциплины модуля и которые должны будут продемонстрированы обучающимися и оценены преподавателем по индикаторам/измеряемым критериям. Результаты обучения формулируются глаголами в активной форме или отглагольным существительным, должны содержать индикатор/измеряемый критерий (например, самостоятельно формулировать предложения...; понимать/понимание; рассчитывать необходимое количество материалов.../ расчет необходимого количества материалов... и т.д.). При выборе глаголов полезно опираться на таксономию Блума.

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне

обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины.

Индикаторы должны учитываться при выборе и составлении заданий контрольно-оценочных мероприятий (оценочных средств) текущей и промежуточной аттестации.

Таблица 2

| Код и наименование компетенции  | Планируемые результаты обучения (индикаторы)<br>[указываются в соответствии с содержанием трудовых функций из профессиональных стандартов (трудовыми действиями, необходимыми знаниями и умениями), соотносящимися с компетенцией]  |   |   |  |
|---|---|---|---|--|
|   | Знания:   | Умения:   | Практический опыт, владение   | Другие результаты<br>(указываются при необходимости, к примеру, личностные качества) |
| ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; | <p>РО1-3 ОПК1<br/>Знает сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства</p> <p>"РО2-3 ОПК1<br/>Знает психологические аспекты информационной безопасности в современном обществе"</p> <p>"РО3-3 ОПК1<br/>Знает угрозы и источники угроз информационной безопасности современного общества" "</p> | <p>РО1-У ОПК1<br/>Умеет применять основные методы обеспечения информационной безопасности</p> | <p>РО1-В ОПК 1<br/>Владеет базовой терминологией и гуманитарными аспектами в области информационной безопасности личности, общества и государства</p> |  |

|  |  |  |  |  |
|--|--|--|--|--|
|  | Р04-3 ОПК1<br>Знает основные<br>методы<br>обеспечения<br>информационной<br>безопасности" |  |  |  |
|--|--|--|--|--|

### **1.5. Форма обучения**

Обучение по дисциплинам модуля может осуществляться в очной форме

## **2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ**

**ПРОГРАММА МОДУЛЯ**  
*Основы информационнорй безопасности*

**РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН  
МОДУЛЯ**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1**

*Основы информационнорй безопасности*

Рабочая программа дисциплины составлена авторами:

| <b>№ п/п</b> | <b>Фамилия Имя Отчество</b>     | <b>Ученая степень,<br/>ученое звание</b> | <b>Должность</b> | <b>Подразделение</b>                 |
|--------------|---------------------------------|--|------------------|--------------------------------------|
| 1            | Бакланов Валентин<br>Викторович | к.т.н., доцент                           | Доцент           | <i>Радиоэлектроник<br/>и и связи</i> |

**Рекомендовано учебно-методическим советом института радиоэлектроники и информационных технологий - РТФ**

## 2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 1

### *Основы информационной безопасности*

#### 2.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология (*ориентирована на передачу знаний и умений, обеспечивающая усвоение обучающимися содержания обучения, проверку и оценку его качества на репродуктивном уровне*);

#### 2.2. Содержание дисциплины 1

Таблица 1.3

| Код раздела, темы | Раздел, тема дисциплины*   | Содержание   |
|-------------------|--|--|
| 1                 | Информационная безопасность в системе национальной безопасности Российской Федерации | Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутривластная, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.  |
| 2                 | Информационная война, методы и средства ее ведения                                   | Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России. Угрозы информационному обеспечению государственной политики Российской Федерации. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности.<br>Информационная безопасность и информационное |

|  |  |  |
|--|--|--|
|  |  | проти- воборство. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информа- онное оружие, его классификация и возможности. |
|--|--|--|

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

## 2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

*Основы информационнорй безопасности*

### Электронные ресурсы (издания)

- ЭБС, на которые есть подписка,
- [elar.urfu.ru](http://elar.urfu.ru),
- [study.urfu.ru](http://study.urfu.ru),
- иные сайты в домене [urfu.ru](http://urfu.ru).

Сведения берутся из электронного каталога библиотеки

<http://lib.urfu.ru/course/view.php?id=76> и включаются в рабочую программу после проверки их доступности (должен открываться полный текст, а не ознакомительный фрагмент).]

### Печатные издания

1. Бакланов В.В. Введение в информационную безопасность. Направления информационной защиты : курс лекций : учеб. пособие для вузов / В. В. Бакланов .— Екатеринбург : Изд-во Уральского университета, 2007 .— 232 с. — (Приоритетный национальный проект "Образование") (Математика. Компьютерные науки) .— Библиогр.: с. 229-232 .— ISBN 5-7996-0259-5.

2. Расторгуев С.П. Основы информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" и "Информ. безопасность телекоммуникац. систем" / С. П. Расторгуев .— Москва : Академия, 2007 .— 188 с. ; 22 см .— (Высшее профессиональное образование, Информационная безопасность) .— Слов. терминов: с. 182-185. — Библиогр.: с. 180-181 (39 назв.). — Допущено в качестве учебного пособия. — ISBN 978-5-7695-3098-2.

*Дополнительная литература:*

3. Галатенко, В. А. Основы информационной безопасности : Курс лекций: Учеб. пособие для вузов / В. А. Галатенко ; Под ред. В. Б. Бетелина .— 2-е изд., испр. — М. : Интернет- Ун-т Информ. Технологий, 2004 .— 264 с. — (Основы информационных технологий).

— Рек. Учеб.-метод. об-нием в обл. прикладной информатики .— Библиогр.: с. 256-260.

— ISBN 5-9556-0015-9 : 200-00.

4. Основы информационной безопасности : учеб. пособие для вузов / Е. Б. Белов [и др.].

— М.: Горячая линия-Телеком, 2006 .— 544 с. : ил. — Допущено М-вом образования и науки РФ .— ISBN 5-93517-292-5.

б) нормативные правовые акты и стандарты

Документы - Официальный сайт Федеральной службы по техническому и экспортному контролю <http://www.fstec.ru>



Банк данных угроз безопасности информации - Официальный сайт Федеральной службы по техническому и экспортному контролю <http://www.fstec.ru>

[Библиографические описания бумажных ресурсов из электронного каталога библиотеки <http://lib.urfu.ru/course/view.php?id=76> с указанием имеющегося количества экземпляров (в ЗНБ и/или на кафедре или ином подразделении УрФУ) – суммарное количество экземпляров должно быть **не менее 0,25 экземпляра** каждого из изданий, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль), проходящих соответствующую практику]

## Профессиональные базы данных, информационно-справочные системы

### Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

### Базы данных, информационно-справочные и поисковые системы

1. <http://www.intuit.ru/> - Национальный открытый университет «ИНТУИТ»
2. <http://www.edu.ru/> - Федеральный портал. Российское образование.
3. <http://study.urfu.ru> –портал информационно-образовательных ресурсов УрФУ
4. <http://rtf.urfu.ru> - официальный сайт ИРИТ-РтФ

## 2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

*Основы информационнорй безопасности*

**Сведения об оснащённости дисциплины специализированным и лабораторным оборудованием и программным обеспечением**

Таблица 3.1

| № п/п | Виды занятий  | Оснащённость специальных помещений и помещений для самостоятельной работы   | Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа   |
|-------|---|---|--|
|       | Лекции; Практические занятия;<br>Консультации;<br>Самостоятельная работа студентов; | <ol style="list-style-type: none"> <li>1. Компьютерный класс.</li> <li>2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.</li> <li>3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.</li> <li>4. Общесистемное и прикладное программное обеспечение, средства защиты информации:</li> </ol> | <ol style="list-style-type: none"> <li>1. Microsoft Windows 7 Enterprise SP1, Windows Server 2008 R2 Enterprise;</li> <li>2. Microsoft Windows XP SP3, Microsoft Windows Server 2003 R2 Enterprise;</li> <li>3. Microsoft Internet Information Services 6.0.</li> <li>4. Программное обеспечение Microsoft Office версии не менее 2010.</li> </ol> |