

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.И. Князев
С.Т. Князев
27 апреля 2021 г.



РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля
1156868

Модуль
Управление информационной безопасностью

Екатеринбург, 2021

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

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Управление информационной безопасностью

1.1. Аннотация содержания модуля

Модуль «Управление информационной безопасностью» систематизирует информацию в области правового регулирования отношений в информационной сфере, развиваются практические приемы управления организационной структурой обеспечения информационной безопасности на предприятии.

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.	Организационное и правовое обеспечение информационной безопасности	3/108
2	Основы управленческой деятельности в области информационной безопасности	3/108
ИТОГО по модулю:		6/216

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	<i>Информационные технологии, Основы информационной безопасности</i>
Постреквизиты и корреквизиты модуля	<i>Защита информации в информационно-управляющих системах</i>

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)			
	Знания:	Умения:	Практический опыт, владение	Другие результаты (указываются при необходимости, к примеру, личностные качества)
УК-3 – Способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	<p>З-1 — общие формы организации деятельности коллектива;</p> <p>З-2 — психологию межличностных отношений в группах разного возраста;</p> <p>З-3 — основы стратегического планирования работы коллектива для достижения поставленной цели;</p>	<p>У-1 — создавать в коллективе психологически безопасную доброжелательную среду;</p> <p>У-2 — учитывать в своей социальной и профессиональной деятельности интересы коллег;</p> <p>У-3 — предвидеть результаты (последствия) как личных, так и коллективных действий;</p> <p>У-4 — планировать командную работу, распределять поручения и делегировать полномочия членам команды;</p>	<p>П-1 — навыками постановки цели в условиях командой работы;</p> <p>П-2 — способами управления командной работой в решении поставленных задач;</p> <p>П-3 – навыками преодоления возникающих в коллективе разногласий, споров и конфликтов на основе учета интересов всех сторон.</p>	

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной форме

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

ПРОГРАММА МОДУЛЯ
Управление информационной безопасностью

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1
Организационное и правовое обеспечение информационной безопасности

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	К.т.н., доцент	доцент	<i>Учебно-научный центр «Информационна я безопасность»</i>

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Организационное и правовое обеспечение 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	Основные положения государственной политики в сфере обеспечения информационной безопасности	Основы и содержание информационной безопасности; субъекты и объекты правоотношений в сфере ее обеспечения. Доктрина информационной безопасности РФ. Национальные интересы РФ в информационной сфере и их обеспечение. Виды и источники угроз информационной безопасности РФ
2	Принципы правового регулирования отношений и основные понятия в сфере информации, информационных технологий и защиты информации. Ограничение доступа к информации	Конституционные гарантии интересов личности в информационной сфере. Законодательная база обеспечения ИБ. Разделение информации по категориям доступа. Конфиденциальность информации. Виды информации ограниченного доступа и режимы ее защиты. Разделение информации по категориям доступа. Конфиденциальность информации. Виды информации ограниченного доступа и режимы ее защиты: коммерческая тайна, банковская тайна, налоговая тайна, тайна связи, врачебная тайна. Ответственность за нарушение защиты информации ограниченного доступа
3	Правовое регулирование распространения информации	Разделение информации в зависимости от порядка ее предоставления или распространения. Общедоступная информация, распространение которой ограничено или запрещено и ее виды. Понятие организатора распространения информации в сети «Интернет» и его обязанности. Процедуры ограничения доступа к противозаконно распространяемой информации с использованием информационно-телекоммуникационных сетей. Обеспечение доступа к информации о деятельности государственных органов и органов местного самоуправления

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление информационной безопасностью ИСПДн, ГИС и значимых объектов КИИ

Электронные ресурсы (издания)

- ЭБС, на которые есть подписка,

- elar.urfu.ru,
- study.urfu.ru,
- *иные сайты в домене 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. Курило А.П. Основы управления информационной безопасностью : учебное пособие для вузов. — 2-е изд., испр. / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — М. : Горячая линия-Телеком, 2014. — 244 с.: ил. — (Вопросы управления информационной безопасностью. Выпуск 1).

2. Милославская Н.Г. Управление рисками информационной безопасности : учебное пособие для вузов. — 2-е изд., испр. / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — М. : Горячая линия-Телеком, 2014. — 130 с.: ил. — (Вопросы управления информационной безопасностью. Выпуск 2).

Дополнительная литература:

3. Аверченков В.И. Аудит информационной безопасности : учеб. пособие для вузов. — М. : ФЛИНТА, 2011 — 269 с.

4. Аверченков В. И. Аудит информационной безопасности органов исполнительной власти : учеб. пособие / В. И Аверченков, М.Ю. Рытов, А.В. Кувылкин, М.В. Рудановский. — М. : ФЛИНТА, 2011. — 100 с. — Электронный ресурс. Режим доступа : <http://mybrary.ru/users/personal/read/audit-informatsionnoy-bezopasnosti-organov-ispolnitelnoy-vlasti-3-izdanie/>.

5. Астахов А.М. Искусство управления информационными рисками — М. : ДМК Пресс, 2010. — 312 с. — Электронный ресурс. Режим доступа : <http://mybrary.ru/users/personal/read/iskusstvo-upravleniya-informatsionnyimi-riskami/>.

6. Галатенко В.А. Стандарты информационной безопасности : учебное пособие. — 2-е издание / под редакцией академика РАН В.Б. Бетелина. — М. : ИНТУИТ.РУ «Интернет-университет Информационных технологий», 2006. — 264 с.

7. Курило А.П. Аудит информационной безопасности / А.П. Курило, С.Л. Зефирова, В.Б. Голованов и др. — М. : БДЦ-пресс, 2006.—304 с. — Электронный ресурс. Режим доступа : <http://radaread.com/?book=15183&pg=1>

8. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погосин. — М. : Горячая линия-телеком, 2001г. — 148 с. — Электронный ресурс. Режим доступа : <http://bookre.org/reader?file=550028&pg=1>

9. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. — М. : ДМК Пресс, 2004. — 384 с. — Электронный ресурс. Режим доступа : <http://mybrary.ru/users/personal/read/upravlenie-informatsionnyimi-riskami-ekonomicheski-opravdannaya-bezopasnost/>.

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

Стандарты - Интернет портал <https://docs.cntd.ru>

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.ustu.ru> –портал информационно-образовательных ресурсов УрФУ

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление информационной безопасностью ИСПДн, ГИС и значимых объектов КИИ

Сведения об оснащении дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
	Лекции; Практические занятия; Консультации; Самостоятельная работа студентов;	<ol style="list-style-type: none">1. <i>Компьютерный класс.</i>2. <i>Персональный компьютер преподавателя с мультимедиа-проектором и экраном.</i>3. <i>Сертифицированный программно-аппаратный комплекс межсетевого экранирования.</i>4. <i>Общесистемное и прикладное программное обеспечение, средства защиты информации:</i>	<ol style="list-style-type: none">1. Microsoft Windows 7 Enterprise SP1, Windows Server 2008 R2 Enterprise;2. Microsoft Windows XP SP3, Microsoft Windows Server 2003 R2 Enterprise;3. Microsoft Internet Information Services 6.0.4. Программное обеспечение Microsoft Office версии не менее 2010.

ПРОГРАММА МОДУЛЯ
Управление информационной безопасностью

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 2

Основы управленческой деятельности в области информационной безопасности

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Пономарева Ольга Алексеевна		Старший преподаватель	<i>Учебно-научный центр «Информационная безопасность»</i>
2	Макарова Ольга Сергеевна		Старший преподаватель	<i>Учебно-научный центр «Информационная безопасность»</i>

Рекомендовано учебно-методическим советом института радиозлектроники и информационных технологий - РТФ

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 2 *Основы управленческой деятельности в области 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

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Лицензирование и сертификация в сфере информационной безопасности	Виды лицензируемой деятельности в области защиты информации. Порядок и системы лицензирования. Сертификация (подтверждение соответствия) средств защиты информации и защищенных автоматизированных систем. Системы и порядок сертификации ФСТЭК и ФСБ России
2	Преступления в сфере компьютерной информации	Понятие об информационных и компьютерных преступлениях. Компьютер как орудие преступления. Компьютер как средство преступления и хранилище информации о преступной деятельности. Компьютер как предмет преступления. Понятие компьютерной информации. Составы преступлений, предусмотренные ст. 272 – 274.1 УК РФ
3	Понятие критической информационной инфраструктуры Российской Федерации	Понятие критической информационной инфраструктуры Российской Федерации (КИИ). Принципы обеспечения безопасности КИИ. ФЗ 187. Понятия объектов и субъектов КИИ. Категорирование объектов КИИ. Понятия АСУ, компьютерной атаки и компьютерного инцидента. Полномочия Президента и Правительства РФ в сфере обеспечения безопасности КИИ. Полномочия ФСТЭК и ФСБ России в сфере обеспечения безопасности КИИ

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ Основы управленческой деятельности в области информационной безопасности

Электронные ресурсы (издания)

- ЭБС, на которые есть подписка,
- *elar.urfu.ru*,
- *study.urfu.ru*,
- *иные сайты в домене urfu.ru*.

Печатные издания

1. Арчибальд Р. *Управление высокотехнологичными программами и проектами.* / Пер. с англ. – М.: ДМК Пресс, 2010. – 464 с.
2. Бабаскин С.Я. *Инновационный проект: методы отбора и инструменты анализа рисков: Учебное пособие - ("Образовательные инновации").* – М.: Дело АНХ, 2010. – 220 с.
3. Верзух Э. *Управление проектами: Ускоренный курс по программе MBA.* – М.: ИД Вильямс, 2010. – 480 с.

4. Лапина С. Н. Информационные технологии в менеджменте: учебное пособие / С.Н.Лапина, Н. И. Тебайкина. – Екатеринбург : УрФУ, 2014.
5. Ильшева М. А. Управление проектами : учебное пособие / М.А. Ильшева. – Екатеринбург : УрФУ, 2009. – 126 с.

5.1.2. Дополнительная литература

1. Агарков С.А., Кузнецова Е.С., Грязнова М.О. Инновационный менеджмент и государственная инновационная политика. – М.: Академия Естествознания, 2011. – 143 с.
2. Бушуев С.Д. и др. Креативные технологии управления проектами и программами. – Киев: Саммит-книга, 2010, - 768 с.
3. Вишняков Я.Д., Радаев Н.Н. Общая теория рисков: учеб. пособие для студ. высш. учеб. заведений. - М.: Издательский центр "Академия", 2007. - 368 с.
4. Гребенкин А.В., Шкурко В.Е. Возможности и риски в системе управления инновационными проектами организационного развития // Экономика региона. - 2008. - №2. - С. 194-198.
5. Гребенкин А.В., Шкурко В.Е. Управление проектами: риски и модели. Часть 2: Экономико-математическое моделирование системы управления рисками проектов (Препринт). Екатеринбург: Изд-во Урал. Ун-та, 2007. – 72 с.

Профессиональные базы данных, информационно-справочные системы

<http://lib.urfu.ru/mod/data/view.php?id=1379>

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.ustu.ru> –портал информационно-образовательных ресурсов УрФУ

2.4. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 2

Основы управленческой деятельности в области информационной 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; Лабораторные занятия; Консультации; Самостоятельная работа студентов;	<ol style="list-style-type: none"> 1. Компьютерный класс. 2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном. 3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования. 4. Общесистемное и прикладное программное обеспечение, средства защиты информации 	<ul style="list-style-type: none"> • Компьютер, на котором установлено программное обеспечение: MS Excel, Project Expert 7, MS Project.