



Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

Начальник УРОПС
В.А. Мельникова

Рабочая программа модуля

МОДУЛЬ 2. «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ (АСУТП)»

основной профессиональной образовательной программы специалитета
по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ

Цифровых технологий

ВЫПУСКАЮЩАЯ КАФЕДРА

Кафедра информационной безопасности

РАЗРАБОТЧИК

УРОПС

1 ЦЕЛЬ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ

1.1 Цели освоения модуля Модуль 2. «Информационная безопасность автоматизированных систем управления технологическими процессами (АСУТП)».

Целью освоения дисциплины «Организационное обеспечение информационной безопасности АСУТП» является: формирование у студентов теоретических знаний о необходимом комплексе мер информационной безопасности, организационной структуре АСУ ТП, вероятных угрозах и внешних воздействиях на такие системы; развитие у студентов практических навыков и умений по организации и поддержанию выполнения комплекса мер информационной безопасности.

Целью освоения дисциплины «Кибербезопасность АСУТП» является: изучение принципов построения систем защиты информации в АСУТП, способов защиты от угроз безопасности в АСУТП.

Целью освоения дисциплины «Искусственный интеллект в АСУТП» является: сформировать у студентов системное базовое представление об использовании инженерии знаний и нейроинформатики при обеспечении информационной безопасности в автоматизированных системах управления технологическими процессами (АСУТП).

1.2 Процесс изучения модуля направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данной специальности.

Таблица 1 – Планируемые результаты обучения по дисциплинам (модулям), соотнесенные с установленными компетенциями

Код и наименование компетенции	Дисциплины	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями
ПК-1 Способен разрабатывать проектные решения по защите информации в автоматизированных системах, обеспечивать их внедрение и сопровождение	Организационное обеспечение информационной безопасности АСУТП	<p><u>Знать:</u></p> <ul style="list-style-type: none"> - организационные меры по защите информации; способы и средства защиты информации от несанкционированного доступа и утечки по техническим каналам и контроля эффективности защиты информации. <p><u>Уметь:</u></p> <ul style="list-style-type: none"> - организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем; - формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы. <p><u>Владеть:</u></p> <ul style="list-style-type: none"> - навыками разработки систем защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов
	Кибербезопасность АСУТП	<p><u>Знать:</u></p> <ul style="list-style-type: none"> - нормативные правовые акты в области защиты информации в АСУТП; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации в КИИ и АСУТП; - порядок проектирования АС в защищенном исполнении; - национальные, межгосударственные и международные стандарты в области защиты информации АСУТП. <p><u>Уметь:</u></p> <ul style="list-style-type: none"> - выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; - определять класс защищенности автоматизированных систем и ее составных частей в КИИ, ГИС и АСУТП. <p><u>Владеть:</u></p> <ul style="list-style-type: none"> - анализа характера обрабатываемой информации и определение перечня информации, подлежащей защите в АСУТП; - разработки отчетных документов и разделов технических заданий в КИИ и АСУТП;

Код и наименование компетенции	Дисциплины	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями
	Искусственный интеллект в АСУТП	<p>- разрабатывать части проектной документации на системы защиты автоматизированных систем;</p> <p>- обоснования перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы в КИИ и АСУТП.</p> <p><u>Знать:</u></p> <p>- направления и ограничения применения систем искусственного интеллекта в информационной безопасности при разработке проектных решений по защите информации в автоматизированных системах управления технологическими процессами.</p> <p><u>Уметь:</u></p> <p>- определять содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации в АСУТП и выявлять уязвимости информационно-технологических ресурсов автоматизированных систем.</p> <p><u>Владеть:</u></p> <p>- анализом системы защиты АСУ ТП от кибератак.</p>

2 ТРУДОЁМКОСТЬ ОСВОЕНИЯ, СТРУКТУРА И СОДЕРЖАНИЕ МОДУЛЯ, ФОРМЫ АТТЕСТАЦИИ ПО НЕМУ

Модуль 2. «Информационная безопасность автоматизированных систем управления технологическими процессами (АСУТП)» относится к блоку 1 части, формируемой участниками образовательных отношений, и включает в себя три дисциплины.

Общая трудоемкость модуля составляет 15 зачетных единиц (з.е.), т.е. 540 академических часа (405 астр. часов) контактной и самостоятельной учебной работы студента; работой, связанной с текущей и промежуточной (заключительной) аттестацией по дисциплинам модуля.

Распределение трудоемкости освоения модуля по семестрам, видам учебной работы студента, а также формы контроля приведены ниже.

Таблица 2 - Объем (трудоёмкость освоения) в очной форме обучения и структура модуля

Наименование	Семестр	Форма контроля	з.е.	Акад. часов	Контактная работа					СРС	Подготовка и аттестация в период сессии
					Лек	Лаб	Пр	РЭ	КА		
Организационное обеспечение информационной безопасности АСУТП	9	З	3	108	32		16	5	0,15	54,85	
Кибербезопасность АСУТП	11	З	6	216	40		40	8	0,15	127,85	
Искусственный интеллект в АСУТП	10	Э	6	216	32		48	8	1,25	92	34,75
Итого по модулю:			15	540	104		104	21	1,55	274,7	34,75

Обозначения: Э – экзамен; З – зачет; ДЗ – дифференцированный зачет (зачет с оценкой); КР (КП) – курсовая работа (курсовой проект); контр. – контрольная работа, РГР – расчетно-графическая работа; Лек – лекционные занятия; Лаб - лабораторные занятия; Пр – практические занятия; РЭ – контактная работа с преподавателем в ЭИОС; КА – контактная работа, консультации, инд.занятия, практики и аттестации; СРС – самостоятельная работа студентов

При разработке образовательной технологии организации учебного процесса основной упор сделан на соединение активной и интерактивной форм обучения. Интерактивная форма позволяет студентам проявить самостоятельность в освоении теоретического материала и овладении практическими навыками, формирует интерес и позитивную мотивацию к учебе.

3 УЧЕБНАЯ ЛИТЕРАТУРА И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТА

Учебно-методическое обеспечение модуля приведено в таблицах 3 и 4.

Таблица 3 – Перечень основной и дополнительной литературы

Наименование дисциплин	Основная литература	Дополнительная литература
<p>Организационное обеспечение информационной безопасности АСУТП</p>	<p>1. Аверченков, В. И. Служба защиты информации : организация и управление : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 186 с. : ил., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93356 (дата обращения: 07.06.2024). – Библиогр. в кн. – ISBN 978-5-9765-1271-9. – Текст : электронный.</p> <p>2. Непорожнев, Д. А. Безопасность информационных систем Вооруженных Сил Российской Федерации : учебное пособие / Д. А. Непорожнев, Н. Н. Пантелеев. — Москва : РТУ МИРЭА, 2022 — Часть 1 — 2022. — 196 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/265880 (дата обращения: 08.06.2024). — Режим доступа: для авториз. пользователей.</p>	<p>1. Каширская, Е. Н. Защита информации в информационно - управляющих системах : учебное пособие / Е. Н. Каширская, М. А. Макаров. — Москва : РТУ МИРЭА, 2020. — 67 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167621 (дата обращения: 07.06.2024). — Режим доступа: для авториз. пользователей.</p> <p>2. Папиrowsкая, Л. И. Эксплуатационное обслуживание и безопасность информационных систем на железнодорожном транспорте : учебное пособие / Л. И. Папиrowsкая, Е. А. Часовских, М. Н. Липатова. — Самара : СамГУПС, 2022. — 211 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/379283 (дата обращения: 08.06.2024). — Режим доступа: для авториз. пользователей. Папиrowsкая, Л. И. Эксплуатационное обслуживание и безопасность информационных систем на железнодорожном транспорте : учебное пособие / Л. И. Папиrowsкая, Е. А. Часовских, М. Н. Липатова. — Самара : СамГУПС, 2022. — 211 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/379283 (дата обращения: 08.06.2024). — Режим доступа: для авториз. пользователей.</p> <p>3. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 108 с. — ISBN 978-5-507-47575-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/392402 (дата обращения: 08.06.2024). — Режим доступа: для авториз. пользователей.</p>
<p>Кибербезопасность АСУТП</p>	<p>1. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие / В. С. Пелешенко, С. В. Говорова,</p>	<p>1. Расследование инцидентов информационной безопасности : учебное пособие / И.Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 113 с.</p>

Наименование дисциплин	Основная литература	Дополнительная литература
	<p>М. А. Лапина. - Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2017. - 86 с. : ил. - URL: https://biblioclub.ru/index.php?page=book&id=467139. - электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация. - Библиогр. в кн. - ~Б. ц. - Текст : электронный.</p> <p>2.Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум"; Москва: ИНФРА-М, 2013. - 416 с.</p> <p>3.Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 "Информ. безопасность автоматизир. систем" всех форм обучения. ч. 1. - Калининград // . - 171 с. - ISBN 978-5-7481-0514-9</p>	<p>2.Национальная безопасность : учебник / В. И. Абрамов, М. А. Газимагомедов, К. К. Гасанов [и др.] ; под ред. К. К. Гасанова, Н. Д. Эриашвили, О. А. Мироновой. – 3-е изд., перераб. и доп. – Москва : Юнити-Дана, 2023. – 288 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700171 (дата обращения: 05.06.2024). – ISBN 978-5-238-03639-7. – Текст : электронный.</p> <p>3.Информационная безопасность распределенных информационных систем: метод. указания по выполнению лабораторных работ для студентов специальности 10.05.03 "Информационная безопасность автоматизированных систем" всех форм обучения / Федер. агентство по рыболовству [и др.]; сост. В. В. Подтопельный. - Калининград : БГАРФ, 2020 - . - Текст : непосредственный. Ч. 1 / сост. В. В. Подтопельный. - 2020. - 61 с.</p> <p>4.Подтопельный, В.В. Информационная безопасность распределенных информационных систем. ЧАСТЬ 2: методические указания по выполнению лабораторных работ для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» всех форм обучения/ В.В. Подтопельный –.(3 авт. л.)</p> <p>5.Подтопельный В.В., Бабаева А.А. Комплексное обеспечение информационной безопасности автоматизированных систем. ЧАСТЬ 1: методические указания по выполнению лабораторных работ для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» всех форм обучения/ В.В. Подтопельный, А.А.Бабаева – Калининград: Изд-во БГАРФ, 2021– 53 с.(3 авт. л.)</p>
Искусственный интеллект в АСУТП	<p>1.Шелухин, О. И. Искусственный интеллект и машинное обучение в кибербезопасности : учебно-методическое пособие / О. И. Шелухин, А. В. Осин, Д. И. Раковский. — Москва : МТУСИ, 2022. — 52 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL:</p>	<p>1.Южаков А.А. Автоматизированное проектирование средств и систем управления : учебное пособие / Южаков А.А.. — Пермь : Пермский национальный исследовательский политехнический университет, 2015. — 213 с. — ISBN 978-5-398-01464-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/108895.html (дата обращения: 31.05.2024). — Режим доступа: для авторизир. Пользователей.</p>

Наименование дисциплин	Основная литература	Дополнительная литература
	<p>https://e.lanbook.com/book/333755 (дата обращения: 31.05.2024). — Режим доступа: для авториз. пользователей.</p> <p>2.Никольский, С. Н. Автоматизация информационного поведения и искусственный интеллект : учебное пособие / С. Н. Никольский. — Москва : РТУ МИРЭА, 2020. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163824 (дата обращения: 31.05.2024). — Режим доступа: для авториз. пользователей.</p>	<p>2.Сырецкий, Г. А. Искусственный интеллект и основы теории интеллектуального управления : учебное пособие / Г. А. Сырецкий. — Новосибирск : НГТУ, [б. г.]. — Часть 1 : Фазисистемы — 2016. — 92 с. — ISBN 978-5-7782-3021-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118268 (дата обращения: 31.05.2024). — Режим доступа: для авториз. пользователей.</p>

Таблица 4 – Перечень периодических изданий, учебно-методических пособий и нормативной литературы

Наименование дисциплин	Периодические издания	Учебно-методические пособия, нормативная литература
<p>Организационное обеспечение информационной безопасности АСУТП</p>	<p>1. Защита информации. Инсайд [Текст] : информационно-методический журнал. - СПб. : ООО "Изд. Дом "Афина", 2004 - . - ISSN 2413-3582. - Выходит раз в два месяца</p> <p>2. Безопасность информационных технологий [Текст] : научно-технический журнал. - М. : Изд-во журнала "Безопасность информационных технологий", 1994 - . - Выходит ежеквартально</p> <p>3. Гражданская защита [Текст] : научно-практический и методический журнал/ центральное издание МЧС России. - М., 1956 - . - ISSN 0869-5881. - Выходит ежемесячно</p>	<p>1. Организационное и правовое обеспечение информационной безопасности : метод. указания по выполнению практ. занятий для студентов специальности 10.05.03 "Информ. безопасность автоматизир. систем" очной формы обучения / Федер. агентство по рыболовству [и др.] ; авт.-сост. А. Г. Жестовский. - Калининград : БГАРФ, 2021. - 67 с. : рис. - Библиогр.: с. 61-67. - ~Б. ц. - Текст : непосредственный.</p> <p>2. Организационное и правовое обеспечение информационной безопасности : метод. указания по орг. и контролю самостоят. работы для студентов специальности 10.05.03 "Информ. безопасность автоматизир. систем" очной формы обучения / Федер. агентство по рыболовству [и др.] ; авт.-сост. А. Г. Жестовский. - Калининград : БГАРФ, 2021. - 34 с. - 189.00 р. - Текст : непосредственный.</p> <p>3. Программно-аппаратные средства обеспечения информационной безопасности : учеб. пособие для студентов высш. учеб. заведений,</p>

Наименование дисциплин	Периодические издания	Учебно-методические пособия, нормативная литература
	<p>4. Информационно-управляющие системы : науч. журн./ учредитель: "Информационно-управляющие системы". - Санкт-Петербург : Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2002 - . - 29 см. - ISSN 1684-8853. - Выходит раз в два месяца. - Текст : непосредственный.</p> <p>5. Морские интеллектуальные технологии : науч. журнал/ учредитель Морские интеллектуальные технологии : Морские интеллектуальные технологии", 2008 - . - с.а-цв. ил. ; 29 см. - ISSN 2073-7173. - Выходит ежеквартально. - URL: http://morintex.ru/. - Текст : электронный.</p>	<p>обучающихся по направлению "Информ. безопасность", по прогр. подгот. бакалавров, магистров, специалистов / А. Г. Жестовский, В. В. Подтопельный ; Федер. агентство по рыболовству [и др.]. - Калининград : БГАРФ, 2018 - . - Текст : непосредственный. Ч. 2 : Настройка систем защиты информации от несанкционированного доступа. - 2018. - 100 с. : ил., табл. - Библиогр.: с. 97-98 (17 назв.). - ISBN 978-5-7481-0389-3 : 211.00 р.</p> <p>Рек. Северо-Зап. регион. отд-нием УМО по информ. безопасности.</p> <p>4. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (выписка в части вопросов защиты информации).</p> <p>5. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (выписка в части вопросов защиты информации).</p> <p>6. Гражданский кодекс Российской Федерации. Часть четвертая. Интеллектуальная собственность.</p> <p>7. Федеральный закон Российской Федерации от 28 декабря 2010 г № 380 - ФЗ "О безопасности".</p> <p>8. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации».</p> <p>9. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».</p> <p>10. Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне»</p> <p>11. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации от 5 декабря 2016 г. № 646.</p> <p>12. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».</p> <p>13. Постановление Правительства РФ от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».</p>

Наименование дисциплин	Периодические издания	Учебно-методические пособия, нормативная литература
		<p>14. Постановление Правительства РФ от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».</p> <p>15. ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.</p> <p>16. ГОСТ Р ИСО/МЭК 18045—2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий;</p> <p>17. ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования.</p> <p>18. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности.</p> <p>19. ГОСТ Р 55.0.02-2014/ИСО 55001:2014 Управление активами. Национальная система стандартов. Системы менеджмента</p>
Кибербезопасность АСУТП		<p>1. "Доктрина информационной безопасности Российской Федерации" (утв. Указом Президентом РФ 05.12.2016 № 646 (в действующей редакции)). - Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.</p> <p>2. "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). - Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.</p> <p>3. Федеральный закон от 28.12.2010 N 390-ФЗ "О безопасности" (в действующей редакции). - Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.</p> <p>4. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (в действующей редакции). - Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.</p>

Наименование дисциплин	Периодические издания	Учебно-методические пособия, нормативная литература
		<p>5. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (в действующей редакции). - Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.</p> <p>6. Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне" (в действующей редакции). - Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.</p> <p>7. Федеральный закон от 15.11.2010 N 299-ФЗ "О внесении изменений в статью 5 Закона Российской Федерации "О государственной тайне" (в действующей редакции). - Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.</p> <p>8. Указ Президента РФ от 06.03.1997 N 188 "Об утверждении Перечня сведений конфиденциального характера" (в действующей редакции). - Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.</p> <p>9. "ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования" (принят и введен в действие Постановлением Госстандарта РФ от 09.02.1995 N 49) (в действующей редакции). - Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.</p> <p>10. "ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения" (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 N 373-ст) (в действующей редакции). - Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.</p> <p>11. "Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" (утв. Решением Гостехкомиссии России от 30.03.1992) (в действующей редакции). - Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.</p>

Наименование дисциплин	Периодические издания	Учебно-методические пособия, нормативная литература
		<p>12. "Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" (утв. Решением Гостехкомиссии России 30.03.1992) (в действующей редакции). - Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.</p> <p>13. ГОСТ Р ИСО/МЭК ТО 18044-2007</p>
Искусственный интеллект в АСУТП	<p>1. Защита информации. Инсайд: информационно-методический журнал. - СПб.: ООО "Изд. Дом "Афина".</p> <p>2. Безопасность информационных технологий: научно-технический журнал. - М.: Изд-во журнала "Безопасность информационных технологий".</p> <p>3. Информационно-управляющие системы = Informatsionno-upravliaiushchie sistemy: науч. журн./ учредитель: "Информационно-управляющие системы"; гл. ред. Михаил Сергеев. - Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2002 -. - 29 см. - Перевод заглавия: Informatsion and control systems. - Срок хранения 5 лет. - Выходит раз в два месяца Гл. ред.: Сергеев М. Б. - ISSN 1684-8853. - Текст: непосредственный. Держатели документа: НТБ КГТУ: 236022, г. Калининград, Советский пр. д. 1</p>	<p>1. Мещерина, Е. В. Системы искусственного интеллекта: учебно-методическое пособие для обучающихся по образовательным программам высшего образования по направлениям подготовки 02.03.01 математика и компьютерные науки, 02.03.02 фундаментальная информатика и информационные технологии, специальности 10.05.01 компьютерная безопасность / Е. В. Мещерина. - Оренбург: ОГУ, 2019. - 96 с. - URL: https://e.lanbook.com/book/160008. - ISBN 978-5-7410-2315-0: ~Б. ц. - Текст: электронный.</p>

4 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНТЕРНЕТ-РЕСУРСЫ МОДУЛЯ

Информационные технологии

В ходе освоения дисциплин модуля, обучающиеся используют возможности интерактивной коммуникации со всеми участниками и заинтересованными сторонами образовательного процесса, ресурсы и информационные технологии посредством электронной информационной образовательной среды университета.

Перечень современных профессиональных баз данных и информационных справочных систем, к которым обучающимся по образовательной программе обеспечивается доступ (удаленный доступ), а также перечень лицензионного программного обеспечения определяется в рабочей программе и подлежит обновлению при необходимости.

Электронные образовательные ресурсы:

Российская образовательная платформа и конструктор бесплатных открытых онлайн-курсов и уроков - <https://stepik.org>

Образовательная платформа - <https://openedu.ru/>

Состав современных профессиональных баз данных (СПБД) и информационных справочных систем (ИСС).

1. Организационное обеспечение информационной безопасности АСУТП

- Полнотекстовая электронная библиотека <http://www.biblioclub.ru>
- Электронная интернет библиотека <http://www.iqlib.ru>
- Опубликованные нормативные-правовые акты РФ <http://www.rg.ru/dok/>
- Правовые аспекты обеспечения информационной безопасности <http://avoidance.ru>
- Правовые и организационно-распорядительные документы по технической защите информации <http://www.altx-soft.ru>
- Библиотека гостей, стандартов и нормативов <http://www.infosait.ru>
- Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) <http://fstec.ru/>
- «Консультант Плюс»; www.consultant.ru
- «Гарант»; www.garant.ru

2. Кибербезопасность АСУТП

- «Консультант Плюс»; www.consultant.ru
- «Гарант»; www.garant.ru
- Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) <http://fstec.ru/>
- Группа компаний «Конфидент» – негосударственная организация в области защиты

информации <http://www.confident.ru>

- Электронная интернет библиотека <http://www.iqlib.ru>
- Полнотекстовая электронная библиотека <http://www.biblioclub.ru>
- Российская образовательная платформа и конструктор бесплатных открытых онлайн-курсов и уроков <https://stepik.org>
- Сайты библиотек вузов в каталоге ИС "Единое окно" window.edu.ru

3. Искусственный интеллект в АСУТП

- <https://www.tadviser.ru>
- <https://www.digital.gov.ru>

5 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ МОДУЛЯ

Аудиторные занятия проводятся в специализированных аудиториях с мультимедийным оборудованием, в компьютерных классах, а также в других аудиториях университета согласно расписанию занятий.

Консультации проводятся в соответствии с расписанием консультаций.

Предэкзаменационные консультации проводятся в аудиториях в соответствии с графиком консультаций.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

При освоении модуля используется программное обеспечение общего назначения и специализированное программное обеспечение.

Перечень соответствующих помещений и их оснащения размещен на официальном сайте университета в информационно - телекоммуникационной сети Интернет.

6 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ АТТЕСТАЦИИ, СИСТЕМА ОЦЕНИВАНИЯ И КРИТЕРИИ ОЦЕНКИ

Типовые контрольные задания и иные материалы, необходимые для оценки результатов освоения дисциплин модуля (в т.ч. в процессе освоения), а также методические материалы, определяющие процедуры этой оценки приводятся в приложении к рабочей программе модуля (утверждается отдельно).

Оценивание результатов обучения может проводиться с применением электронного обучения, дистанционных образовательных технологий.

7 СВЕДЕНИЯ О РАБОЧЕЙ ПРОГРАММЕ И ЕЕ СОГЛАСОВАНИИ

Рабочая программа модуля «Модуль 2. Информационная безопасность автоматизированных систем управления технологическими процессами (АСУТП)» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем».

Рабочая программа рассмотрена и одобрена на заседании методической комиссии института цифровых технологий (протокол № 3 от 23.04.2024)

Председатель методической
комиссии



О.С. Витренко

Директор института



А.Б. Тристанов