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

_____ С.Т. Князев
«___» _____

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля	Модуль
1144713	Информационное обеспечение профессиональной деятельности

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Экономико-правовое обеспечение экономической безопасности	**Код ОП** 1. 38.05.01/33.04
Направление подготовки 1. Экономическая безопасность	**Код направления и уровня подготовки** 1. 38.05.01

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Крылов Виктор Гаврилович	без ученой степени, без ученого звания	Старший преподаватель	региональной экономики, инновационного предпринимательства и безопасности
2	Шкурко Валентина Евгеньевна		старший преподаватель	региональной экономики, инновационного предпринимательства и безопасности

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Информационное обеспечение профессиональной деятельности

1.1. Аннотация содержания модуля

В рамках модуля «Информационное обеспечение профессиональной деятельности» предполагается рассмотреть основные аспекты содержания информационных технологий, отличительной особенностью которой является повышение эффективности профессиональной деятельности. Целью модуля является формирование у студентов компетенций, связанных с основами организации современных информационных технологий и их применения в экономической и управленческой деятельности предприятий, рассмотрение основных принципов построения, внедрения и ведения специализированных информационных систем, создание у студентов целостного представления о процессах формирования информационного общества, а также формирование у студентов знаний и умений в области экономической и компьютерной подготовки, необходимых для успешного применения современных информационных технологий в сфере своей профессиональной деятельности на практике. Дисциплина «Информационная безопасность» охватывает круг вопросов, связанных с изучением основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах. Дисциплина «Технические способы защиты информации» формирует у студентов навыки, необходимые для решения таких профессиональных задач, как проведение мониторинга защищенности объекта; поиск рациональных решений при разработке средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения.

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
1	Информационная безопасность	4
2	Технические способы защиты информации	3
	ИТОГО по модулю:	7

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Информационно-математические основы профессиональной деятельности
Постреквизиты и кореквизиты модуля	Не предусмотрены

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

Таблица 2

Перечень дисциплин модуля	Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
1	2	3
Информационная безопасность	ПК-4 - Способен обеспечивать условия защиты ресурсов организации от внешних и внутренних угроз экономической безопасности	З-1 - Знать понятия внешних и внутренних угроз экономической безопасности З-2 - Знать методики защиты ресурсов организации от внешних и внутренних угроз экономической безопасности У-1 - Уметь применять методики защиты ресурсов организации от внешних и внутренних угроз экономической безопасности П-1 - Владеть методиками защиты ресурсов организации от внешних и внутренних угроз экономической безопасности
Технические способы защиты информации	ПК-4 - Способен обеспечивать условия защиты ресурсов организации от внешних и внутренних угроз экономической безопасности	З-1 - Знать понятия внешних и внутренних угроз экономической безопасности З-2 - Знать методики защиты ресурсов организации от внешних и внутренних угроз экономической безопасности У-1 - Уметь применять методики защиты ресурсов организации от внешних и внутренних угроз экономической безопасности П-1 - Владеть методиками защиты ресурсов организации от внешних и внутренних угроз экономической безопасности

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной и заочной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Крылов Виктор Гаврилович	без ученой степени, без ученого звания	Старший преподаватель	региональной экономики, инновационного предпринимательства и безопасности
2	Шкурко Валентина Евгеньевна		старший преподаватель	региональной экономики, инновационного предпринимательства и безопасности

Рекомендовано учебно-методическим советом института Институт экономики и управления

Протокол № _13_ от _11.06.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Крылов Виктор Гаврилович, Старший преподаватель, региональной экономики, инновационного предпринимательства и безопасности**
- **Шкурко Валентина Евгеньевна, старший преподаватель, региональной экономики, инновационного предпринимательства и безопасности**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Введение	Определение понятия “информационная безопасность”. Информационная безопасность как отрасль. Роль и место информационной безопасности в профессиональной деятельности. Современное состояние и перспективы информационной безопасности. Государственное регулирование в сфере ИБ. Международные нормы и стандарты по ИБ.
Р2	Виды угроз ЭБ	Классификация угроз информации и информационным технологиям. Субъекты ИБ. Угрозы доступности, целостности и конфиденциальности информации. Категории атак на информационные системы. Сценарий типовой атаки на информационную систему. Локальные атаки. Удаленные атаки. Атаки на поток данных. Атаки на пользователя (социальная инженерия).
Р3	Безопасность программного обеспечения	Средства защиты информации и обеспечения безопасности информационных технологий. Определение понятия «уязвимость программного обеспечения». Обзор методик тестирования и выявления уязвимостей. Организационные меры по обеспечению безопасности использования программного обеспечения. Меры защиты и подтверждения авторских прав на разрабатываемое программное обеспечение.

Р4	Встроенные средства безопасности операционных систем	Средства идентификации и аутентификации пользователей. Группы безопасности. Политика регистрации событий. Шифрование. Корпоративная безопасность. Службы сертификации. Встроенный Firewall. Политика ограничения используемых приложений. Средства электронной цифровой подписи. Защита от макровирусов. Централизованные средства управления. Компьютерные вирусы и антивирусные средства. Антивирусное программное обеспечение (АВПО). Обзор технологий и производителей АВПО. Практика применения АВПО. Эшелонированные системы антивирусной защиты. Атаки на АВПО.
Р5	Криптографические методы защиты информации	Шифрование (алгоритмы шифрования). Электронно-цифровая подпись (практика применения). Хэширование. Средства инфраструктуры открытых ключей. Атаки на криптографическую защиту.
Р6	Сетевые средств защиты информации.	Технологии защиты вычислительных сетей. Обзор сетевых средств защиты информации (межсетевые экраны, виртуальные частные сети, шифрование, обнаружение вторжений). Методы применения сетевых СЗИ. Основы безопасной работы в сети Интернет. Безопасность электронной коммерции. Безопасность беспроводных технологий. Стандарты безопасности беспроводных сетей. Меры защиты от различного вида атак. Технологии защиты Wi-Fi-сетей.
Р7	Управление рисками ИБ	Соотношение угроз, уязвимостей и ущерба. Этапы управления рисками. Методики оценки рисков. Методы снижения рисков. Организация системы информационной безопасности предприятия. Построение системы управления информационной безопасности (СУИБ) предприятия. Общие правила безопасности предприятия. Архитектура СУИБ. Настройки основных компонентов СУИБ. Корпоративные политики информационной безопасности

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	целенаправленная работа с информацией для использования в практических целях	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-4 - Способен обеспечивать условия защиты ресурсов организации от внешних и внутренних угроз экономической безопасности	З-1 - Знать понятия внешних и внутренних угроз экономической безопасности З-2 - Знать методики защиты ресурсов организации от внешних и

				внутренних угроз экономической безопасности У-1 - Уметь применять методики защиты ресурсов организации от внешних и внутренних угроз экономической безопасности П-1 - Владеть методиками защиты ресурсов организации от внешних и внутренних угроз экономической безопасности

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Информационная безопасность

Электронные ресурсы (издания)

1. Филиппов, Б. И.; Информационная безопасность. Основы надежности средств связи : учебник.; Директ-Медиа, Москва|Берлин; 2019; http://biblioclub.ru/index.php?page=book&id=499170 (Электронное издание)

2. Ищейнов, В. Я.; Информационная безопасность и защита информации: теория и практика : учебное пособие.; Директ-Медиа, Москва|Берлин; 2020; http://biblioclub.ru/index.php?page=book&id=571485 (Электронное издание)

3. Артемов, А. В.; Информационная безопасность: курс лекций : курс лекций.; Межрегиональная академия безопасности и выживания, Орел; 2014; https://biblioclub.ru/index.php?page=book&id=428605 (Электронное издание)

Профессиональные базы данных, информационно-справочные системы

1. Международная база цитирований Web of Science - https://apps.webofknowledge.com/

2. Международная база цитирований Scopus - https://www.scopus.com/

3. Электронный научный архив УрФУ - http://elar.urfu.ru/

4. Справочно-библиографическая система - http://search.ebscohost.com/

5. Научная электронная библиотека - http://elibrary.ru/

6. Российская государственная библиотека (Москва) – РГБ http://www.rsl.ru/

7. Российская национальная библиотека (Санкт-Петербург) - http://www.nlr.ru/

8. Свердловская областная универсальная научная библиотека им. В.Г. Белинского http://book.uraic.ru/el_library

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. Справочно-правовая система «Консультант Плюс»

2. Справочно-правовая система «Гарант»1. Федеральная служба государственной статистики - https://rosstat.gov.ru/

2. Яндекс.Метрика - https://metrika.yandex.ru

3. Google Analytics - https://analytics.google.com/

3. Справочная система «КонсультантПлюс» www.consultant.ru;

4. Справочная система «Гарант» – www.garant.ru ;

5. Единое окно доступа к образовательным ресурсам – http://window.edu.ru;

6. Официальный сайт Федеральной таможенной службы России – http://www.customs.ru/;

7. Официальный сайт Федеральной службы по защите прав потребителей и благополучия человека – http://www.rospotrebnadzor.ru/;

8. Федеральное агентство по техническому регулированию и метрологии - http://www.interstandart.ru/ официальный сайт информационной службы «Интерстандарт».

9. Система Профессионального Анализа Рынка и Компаний (СПАРК) - http://spark.interfax.ru/.

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Информационная безопасность

Сведения об оснащенности 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
1	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов	Adobe Acrobat Professional 2017 Multiple Platforms M365AppsForEnterpriseEDU ShrdSvr ALNG SubsVL MVL PerUsr

		Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	
2	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Adobe Acrobat Professional 2017 Multiple Platforms M365AppsForEnterpriseEDU ShrdSvr ALNG SubsVL MVL PerUsr
3	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Adobe Acrobat Professional 2017 Multiple Platforms M365AppsForEnterpriseEDU ShrdSvr ALNG SubsVL MVL PerUsr
4	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Adobe Acrobat Professional 2017 Multiple Platforms M365AppsForEnterpriseEDU ShrdSvr ALNG SubsVL MVL PerUsr
5	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Adobe Acrobat Professional 2017 Multiple Platforms M365AppsForEnterpriseEDU ShrdSvr ALNG SubsVL MVL PerUsr

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Технические способы защиты информации

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Крылов Виктор Гаврилович	без ученой степени, без ученого звания	Старший преподаватель	региональной экономики, инновационного предпринимательства и безопасности
2	Шкурко Валентина Евгеньевна		старший преподаватель	региональной экономики, инновационного предпринимательства и безопасности

Рекомендовано учебно-методическим советом института Институт экономики и управления

Протокол № _13_ от _11.06.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Крылов Виктор Гаврилович, Старший преподаватель, региональной экономики, инновационного предпринимательства и безопасности**
- **Шкурко Валентина Евгеньевна, старший преподаватель, региональной экономики, инновационного предпринимательства и безопасности**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Введение. Угрозы в информационных сетях	Основные понятия. Информационная безопасность как отрасль. Роль и место информационной безопасности в профессиональной деятельности. Виды угроз. Внутренние и внешние источники угроз. Организационно-правовое обеспечение информационной безопасности. Современное состояние и перспективы информационной безопасности. Государственное регулирование в сфере ИБ. Международные нормы и стандарты по ИБ. Нарушения конфиденциальности, достоверности, целостности, доступности. Классификация угроз информации и информационным технологиям. Субъекты ИБ. Угрозы доступности, целостности и конфиденциальности информации. Категории атак на информационные системы. Сценарий типовой атаки на информационную систему. Локальные атаки. Удаленные атаки. Атаки на поток данных. Атаки на пользователя (социальная инженерия).
Р2	Безопасность операционных систем и программного обеспечения	Средства защиты информации и обеспечения безопасности информационных технологий. Определение понятия «уязвимость программного обеспечения». Обзор методик тестирования и выявления уязвимостей. Организационные

		меры по обеспечению безопасности использования программного обеспечения. Средства идентификации и аутентификации пользователей. Группы безопасности. Политика регистрации событий. Шифрование. Корпоративная безопасность. Службы сертификации. Встроенный Firewall. Политика ограничения используемых приложений. Средства электронной цифровой подписи. Защита от макровирусов. Централизованные средства управления. Компьютерные вирусы и антивирусные средства. Антивирусное программное обеспечение (АВПО). Обзор технологий и производителей АВПО. Практика применения АВПО. Эшелонированные системы антивирусной защиты. Атаки на АВПО.
Р3	Способы и средства защиты информации	Основные способы и средства защиты информации. Системы защиты информации. Основы криптографии. Терминология и основные понятия криптологии. Основные аспекты криптографии. Основные аспекты криптоанализа. Шеноновские модели криптографии. Теоретико-информационные оценки стойкости симметричных криптосистем. Криптографические методы защиты информации. Компьютерные вирусы и антивирусные программы
Р4	Криптографические методы защиты информации	Основные принципы кодирования. Основы экономного кодирования. Введение в теорию кодирования. Основы экономного кодирования. Сжатие без потерь информации. Сжатие с потерями информации. Кодеры, основанные на системе сжатия без потерь информации. Основные методы побуквенного кодирования. Код Хаффмана. Код Шеннона. Код Шеннона-Фано. Код Гильбера-Мура. Помехоустойчивое кодирование. Коды с обнаружением ошибок. Коды с исправлением ошибок. Линейные блоковые коды. Коды Хэмминга. Циклические коды. Псевдослучайные последовательности. Равномерно распределенная случайная последовательность. Алго-ритмы генерации псевдослучайных последовательно-стей. Конгруэнтные генераторы. Линейные и мульти-пликативные конгруэнтные генераторы. Нелинейные конгруэнтные генераторы. Квадратичные конгруэнтные генераторы. Генератор Эйхенауэра - Лена с обращени-ем. Конгруэнтный генератор, использующий умноже-ние с переносом. Рекуренты в конечном поле. После-довательности, порождаемые линейными регистрами сдвига с обратной связью. Генераторы Фибонначи. Криптостойкие генераторы на основе односторонних функций. Криптостойкие генераторы, основанные на проблемах теории чисел. Методы «улучшения» эле-ментарных псевдослучайных последовательностей. Комбинирование алгоритмов генерации методом Ма-кларена - Марсальи. Комбинирование LFSR-генераторов. Комбинирование с помощью псевдослу-чайного прореживания. Конгруэнтный генератор со случайными параметрами.

		Тестирование чисел на простоту и построение боль-ших простых чисел. Метод пробных делений. Решето Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма. Тест Соловея - Штрассена. Тест Ле-манна. Тест Рабина - Миллера. Полиномиальный тест распознавания простоты. Тест Конягина - Померанса. Метод Михалеску. Теория сравнения Арифметика вычетов. Функция Эй-лера. Сравнение первой степени. Решение сравнения первой степени с использованием алгоритма Евклида. Решение сравнения первой степени с использованием расширенного алгоритма Евклида. Решение сравнения способ Эйлера. Первообразные корни. Дискретные ло-гарифмы в конечном поле. Разложение на множители (факторизация) Метод Ферма. - факторизация Поллар-да. Метод -Полларда. Метод Шермана-Лемана. Метод Ленстры. Примеры систем шифрования, основанные на проблемах теории чисел Система шифрования RSA. Система шифрования Диффи-Хеллмана. Шифрование (алгоритмы шифрования). Электронно-цифровая подпись (практика применения). Хэширование. Средства инфраструктуры открытых ключей. Атаки на криптографическую защиту
Р5	Сетевые средства защиты информации	Технологии защиты вычислительных сетей. Обзор сетевых средств защиты информации (межсетевые экраны, виртуальные частные сети, шифрование, обнаружение вторжений). Методы применения сетевых СЗИ. Основы безопасной работы в сети Интернет. Безопасность электронной коммерции. Безопасность беспроводных технологий. Стандарты безопасности беспроводных сетей. Меры защиты от различного вида атак. Технологии защиты Wi-Fi-сетей
Р6	Управление рисками информационной безопасности	Соотношение угроз, уязвимостей и ущерба. Этапы управления рисками. Методики оценки рисков. Методы снижения рисков. Организация системы информационной безопасности предприятия. Построение системы управления информационной безопасности (СУИБ) предприятия. Общие правила безопасности предприятия. Архитектура СУИБ. Настройки основных компонентов СУИБ. Корпоративные политики информационной безопасности. Стандарты общего назначения, стандарты по криптографической защите. Стандарты, руководящие методические материалы информационной безопасности

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональн	целенаправленна	Технология	ПК-4 - Способен	З-1 - Знать

ое воспитание	я работа с информацией для использования в практических целях	формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	обеспечивать условия защиты ресурсов организации от внешних и внутренних угроз экономической безопасности	понятия внешних и внутренних угроз экономической безопасности З-2 - Знать методики защиты ресурсов организации от внешних и внутренних угроз экономической безопасности У-1 - Уметь применять методики защиты ресурсов организации от внешних и внутренних угроз экономической безопасности П-1 - Владеть методиками защиты ресурсов организации от внешних и внутренних угроз экономической безопасности

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Технические способы защиты информации

Электронные ресурсы (издания)

1. Ищейнов, В. Я.; Информационная безопасность и защита информации: теория и практика : учебное пособие.; Директ-Медиа, Москва|Берлин; 2020; http://biblioclub.ru/index.php?page=book&id=571485 (Электронное издание)

2. Сергеева, Ю. С.; Защита информации: конспект лекций : учебное пособие.; А-Приор, Москва; 2011; https://biblioclub.ru/index.php?page=book&id=72670 (Электронное издание)

3. Титов, А. А.; Инженерно-техническая защита информации : учебное пособие.; Томский государственный университет систем управления и радиоэлектроники, Томск; 2010; https://biblioclub.ru/index.php?page=book&id=208567 (Электронное издание)

4. Прохорова, О. В.; Информационная безопасность и защита информации : учебник.; Самарский

государственный архитектурно-строительный университет, Самара; 2014; https://biblioclub.ru/index.php?page=book&id=438331 (Электронное издание)

Профессиональные базы данных, информационно-справочные системы

1. Международная база цитирований Web of Science - https://apps.webofknowledge.com/

2. Международная база цитирований Scopus - https://www.scopus.com/

3. Электронный научный архив УрФУ - http://elar.urfu.ru/

4. Справочно-библиографическая система - http://search.ebscohost.com/

5. Научная электронная библиотека - http://elibrary.ru/

6. Российская государственная библиотека (Москва) – РГБ http://www.rsl.ru/

7. Российская национальная библиотека (Санкт-Петербург) - http://www.nlr.ru/

8. Свердловская областная универсальная научная библиотека им. В.Г. Белинского http://book.uraic.ru/el_library

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. Справочно-правовая система «Консультант Плюс»

2. Справочно-правовая система «Гарант»1. Федеральная служба государственной статистики - https://rosstat.gov.ru/

2. Яндекс.Метрика - https://metrika.yandex.ru

3. Google Analytics - https://analytics.google.com/

3. Справочная система «КонсультантПлюс» www.consultant.ru;

4. Справочная система «Гарант» – www.garant.ru ;

5. Единое окно доступа к образовательным ресурсам – http://window.edu.ru;

6. Официальный сайт Федеральной таможенной службы России – http://www.customs.ru/;

7. Официальный сайт Федеральной службы по защите прав потребителей и благополучия человека – http://www.rospotrebnadzor.ru/;

8. Федеральное агентство по техническому регулированию и метрологии - http://www.interstandart.ru/ официальный сайт информационной службы «Интерстандарт».

9. Система Профессионального Анализа Рынка и Компаний (СПАРК) - http://spark.interfax.ru/.

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Технические способы защиты информации

Сведения об оснащенности 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
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Adobe Acrobat Professional 2017 Multiple Platforms M365AppsForEnterpriseEDU ShrdSvr ALNG SubsVL MVL PerUsr
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Adobe Acrobat Professional 2017 Multiple Platforms M365AppsForEnterpriseEDU ShrdSvr ALNG SubsVL MVL PerUsr
3	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Adobe Acrobat Professional 2017 Multiple Platforms M365AppsForEnterpriseEDU ShrdSvr ALNG SubsVL MVL PerUsr
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов	Adobe Acrobat Professional 2017 Multiple Platforms

		Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	M365AppsForEnterpriseEDU ShrdSvr ALNG SubsVL MVL PerUsr
5	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Adobe Acrobat Professional 2017 Multiple Platforms M365AppsForEnterpriseEDU ShrdSvr ALNG SubsVL MVL PerUsr