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
29 апреля 2021 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля	**Модуль**
1157113	*Методы расследования преступлений в сфере информационных технологий*

Екатеринбург, 2021

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа *Информационно-аналитические системы безопасности*	**Код ОП 10.05.04/22.01**
Направление подготовки Информационная безопасность	**Код направления и уровня подготовки** *10.05.04*

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	*специалитет*

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	*Учебно-научный центр «Информационная безопасность»*
2	Пономарева Ольга Алексеевна		Старший преподаватель	*Учебно-научный центр «Информационная безопасность»*

Руководитель модуля - *С.В. Поршнев*

Согласовано:

Управление образовательных программ Р.Х.Токарева

ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Методы расследования преступлений в сфере информационных технологий

1.1. Аннотация содержания модуля

Модуль «Методы расследования преступлений в сфере информационных технологий» предназначен для теоретического и практического обучения студентов с комплексом методов и средств по раскрытию возможных преступлений совершенных с применением информационных технологий

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.	Методы расследования компьютерных преступлений	*6/216*
2	Методы расследования финансовых преступлений в сфере информационных технологий	*3/108*
	ИТОГО по модулю:	*9/324*

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	- *Управление информационной безопасностью* - *Методы резервирования и восстановления информации* - *Безопасность файловых систем* - *Методы и средства защиты информации в объектах КИИ* - *Математические методы теории сигналов и систем* - *Управление проектами в области информационной безопасности* -*Управление рисками в области информационной безопасности* - *Аудит банковский операций* - *Информационная безопасность банковских операций*
Постреквизиты и корреквизиты модуля	*Нет*

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) [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** *(указываются при необходимости, к примеру,* ***личностные качества)***
УК- 10. Способен формировать нетерпимое отношение к коррупционному поведению	З-1 - Описывать основные права и обязанности человека и гражданина и способы воспитания нетерпимого отношения к коррупции в различных областях жизнедеятельности З-2 - Характеризовать законодательные нормы, направленные на борьбу с коррупционным	У-1 - Распознавать признаки коррупционного поведения в различных областях жизнедеятельности и определять свою жизненную позицию на основе гражданских ценностей, социальной ответственности и нетерпимости к коррупции У-2 - Оценивать политические и социально-экономические	П-1 - Иметь опыт решения проблемных ситуаций, связанных с коррупционным поведением граждан, нарушением гражданских прав, применением манипулятивных технологий формирования ложных и антиправовых действий, опираясь на законодательные	

	поведением, манипулятивные технологии формирования ложных и антиправовых действий	события и ситуации, выявлять действия, направленные на манипулирование людьми, и определять способы противостояния психологической манипуляции	нормы и собственную позицию нетерпимого отношения к коррупции	

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной форме

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

ПРОГРАММА МОДУЛЯ

Методы расследования преступлений в сфере информационных технологий

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

Методы расследования финансовых преступлений в сфере информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бакланов Валентин Викторович	К.т.н., доцент	доцент	*Учебно-научный цент р «Информационна я безопасность»*

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 1

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, внутриполитическая, 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. 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. Информационная безопасность и информационное противоборство. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности.

3	Платежные терминалы	Классификация платежных терминалов по функциональным возможностям. Агентская и банковская схемы функционирования. Функциональные части и их назначение. Корпус платежного терминала, модем для организации обмена информацией между платежным терминалом и сервером электронной платежной системы. Конструктивные особенности Безопасность платежных терминалов. Этапы работы платежных терминалов.
4	Основные виды угроз в отношении Банкоматов и платежных терминалов	Общие критерии формирования модели нарушителя. Типология нарушителей. Категории нарушителей и виды совершаемых преступлений. Цели нарушителей. Оценка опасности нарушителя исходя из степени его осведомленности, оснащенности и подготовленности, типология нарушителей по подготовленности к преодолению системы охраны. Категории нарушителей и виды совершаемых ими преступлений, связанных с незаконным проникновением в зону размещения банкоматов и 7 платежных терминалов, криминальными посягательствами и конфиденциальную информацию банкоматов, а также на пользователей платежных терминалов и банкоматов, инкассаторов и обслуживающий персонал. Квалификация преступления. Угрозы держателю карты, обслуживающему персоналу. Нападение. Неправомерный доступ к Персональным данным. Угрозы банковской карте, ее реквизитам. Скимминг. Шимминг. Траппинг. Угрозы банкоматам и платежным терминалам. Несанкционированное проникновение на территорию, в здание, где установлены платежные терминалы и банкоматы. Вскрытие банкоматов. Хищение, срыв с места установки.
5	Обеспечение безопасности платежных терминалов и банкоматов	Требования Положения ЦБ РФ по обеспечению безопасной эксплуатации платежных терминалов и банкоматов. Основные организационные и технические меры по защите информации банкоматов и платежных терминалов. Выбор мест размещения банковских устройств самообслуживания. Влияние категории на место размещения. Анализ уязвимостей программного обеспечения банкоматов и терминалов. Обеспечение фиксации. Инженерно-техническая укрепленность и оборудование техническими средствами охраны банковских устройств самообслуживания и мест их размещения. Регулирование и установка порядков срока хранения информации, обновления версий, работы с клиентами. Оценка времени взлома. Минимальные требования по устойчивости к

		взлому сейфов. Системы удаленного мониторинга состояния устройства, обеспечивающие контроль надлежащего функционирования защитного оборудования и специального программного обеспечения. Требования к системе передачи тревожных сообщений для защиты банкоматов и платежных терминалов. Фиксация фактов атак и попыток их совершения. Информирование Банка России. Информирование населения.

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. Мошенничество в платежной сфере: бизнес-энциклопедия / Центр исследований 12 платежных систем и расчетов ; ред.-сост. А. Воронин. - Москва : Интеллектуальная Литература, 2016. - 345 с. : табл., схем. - ISBN 978-5-99072-232-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=430951

2. Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605

3. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стереотип. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93245

4. Аудит информационной безопасности органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. - 4-е изд., стереотип. - Москва : Издательство «Флинта», 2016. - 100 с. - (Организация и технология защиты информации). - Библиогр.: с. 83-84. - ISBN 978-5-9765-1277-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93259

5. Башлы, П.Н. Информационная безопасность : учебно-практическое пособие / П.Н. Башлы, Е.К. Баранова, А.В. Бабаш. - Москва : Евразийский открытый институт, 2011. - 375 с. - ISBN 978-5-374-00301-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90539

Профессиональные базы данных, информационно-справочные системы

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.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

[*список с указанием наименования баз данных, информационно-справочных и поисковых систем*]

www.consultant.ru. - www.garant.ru. - Электронно- библиотечная **система** ZNANIUM.COM – режим доступа www.znanium.com.

- Научная электронная библиотека eLIBRARY.RU – режим доступа http://elibrary.ru.
- Электронная библиотека Grebennikon – режим доступа http://grebennikon.ru/.
- Универсальная справочно-информационная полнотекстовая **база данных** периодических изданий EastViewhttp://ebiblioteka.ru/.

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление информационной безопасностью ИСПДн, ГИС и значимых объектов КИИ

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
	Лекции; Практические занятия; Консультации; Самостоятельная работа студентов;	*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:*	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

Методы расследования преступлений в сфере информационных технологий

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 2

Методы расследования компьютерных преступлений

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бакланов Валентин Викторович	К.т.н., доцент	Доцент	*Учебно-научный центр «Информационная безопасность»*

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 2

Управление проектами 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	Понятие, виды и особенности компьютерных преступлений	Понятие об информационных и компьютерных преступлениях. Особенности и причины информационных преступлений. Понятие о неправомерном обороте информации. Составы информационных преступлений, предусмотренные Уголовным кодексом РФ. Преступления в форме незаконного распространения, разглашения и передачи информации. Незаконное воспрепятствование доступу к информации. Незаконное хранение и использование конфиденциальной информации. Формы информационной фальсификации. Компьютерные мошенничества. Особенности компьютерных преступлений. Преступления в сфере компьютерной информации. Место компьютерных систем в преступной деятельности. Компьютер как непосредственное орудие преступления. Компьютер как средство преступления и хранилище информации о преступной деятельности. Компьютер как предмет преступления.
2	Криминалистическая характеристика преступлений в сфере компьютерной информации	Особенности подготовки компьютерных преступлений. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Виды ЭВМ по отношению к преступной деятельности. Способы нарушения работы ЭВМ, системы ЭВМ и их сети. Формы несанкционированного копирования, удаления, модификации и блокирования защищаемой законом компьютерной информации. Ответственность за совершение преступлений, предусмотренных ст. 272 – 274 УК РФ. Ст. 138 УК РФ - нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений – характеристика и ответственность за совершение преступления. Ст. 159, п. 6 УК РФ - мошенничество в сфере компьютерной информации. – характеристика и ответственность за совершение преступления. Ст. 183 УК РФ - незаконные получение и разглашение сведений, составляющих коммерческую, налоговую

		или банковскую тайну - характеристика и ответственность за совершение преступления.
3	Следовая картина компьютерных преступлений	Машинные носители информации как место нахождения компьютерной информации. Следы криминальной деятельности на машинных носителях. Признаки воздействия на информацию.
4	Организация расследования	Составляющие части расследования. Краткая характеристика составляющих частей расследования. Особенности расследования компьютерных преступлений. Программа расследования на первоначальном этапе. Тактические особенности проведения ОМП. Программа расследования на последующем и завершающем этапах.
5	Следственные ситуации и их разрешения в ходе предварительного расследования	Классификация следственных ситуаций по источнику информации. Классификация следственных ситуаций по объему информации, имеющийся в распоряжении следствия. Ход проведений предварительной и основной проверок. Схемы проведений проверок.
6	Организация и проведение осмотра происшествия	Понятие осмотра места происшествия. Организация осмотра места происшествия. Тактические приемы осмотра места происшествия. Фиксация хода и результатов осмотра места происшествия. Оперативно-розыскные мероприятия примыкающие к осмотру места происшествия.
7	Осмотр средств компьютерной техники	Протокол осмотра средств компьютерной техники. Требования при осмотре средств компьютерной техники. Интересующие сведения при осмотре компьютерной техники. Правила обращения с компьютерной техникой. Цели осмотра компьютерной техники. Осмотр документов учета работы на компьютерной технике.
8	Производство обыска и выемки средств компьютерной техники	Криминалистические цели и задачи производства обыска и выемки в процессе расследования преступлений в сфере компьютерной безопасности. Тактика подготовки к производству обыска и выемки в процессе расследования преступлений в сфере компьютерной безопасности. Тактика производства обыска и выемки в процессе расследования преступлений в сфере компьютерной безопасности. Фиксация хода и результатов обыска и выемки в процессе расследования преступлений в сфере компьютерной безопасности
9	Использование специальных познаний. Судебная компьютернотехническая экспертиза.	Компетенции эксперта в области информационной безопасности. Классификация объектов компьютерной экспертизы. Аппаратные, программные и информационные объекты. Методика экспертизы аппаратных, программных и информационных объектов. Методика экспертизы целостной компьютерной системы, устройства. Виды компьютернотехнической экспертизы специальных средств.

10	Допрос подозреваемых, обвиняемых и свидетелей по делам о компьютерных преступлениях	Понятие, сущность и задачи и значение допроса по делам о компьютерных преступлениях. Организация вызова свидетелей для производства следственных действий. Подготовка к допросу. Составление плана проведения следственного действия. Классификация тактических приемов допроса. Тактические приемы допроса подозреваемого и свидетеля. Фиксация хода и результатов допроса
11	Судебные ситуации и их разрешение в ходе судебного следствия по компьютерным преступлениям.	Понятие судебной ситуации. Специфика и роль судебных ситуаций в криминалистике. Виды судебных ситуаций и алгоритмы их разрешения. Типичные и конкретные судебные ситуации.
12	Криминалистическое предупреждение компьютерных преступлений. Меры обеспечения криминалистического предупреждения	Понятие криминалистического предупреждения компьютерных преступлений. Задачи криминалистического предупреждения криминалистических преступлений. Разработка средств, приемов и методов предупреждения компьютерных преступлений. Классификация обстоятельств, способствующих совершению преступлений в сфере компьютерной информации. Обстоятельства, способствующие к неправомерному доступу к компьютерной информации. Обстоятельства, способствующие созданию, использованию и распространению вредоносных программ для ЭВМ. Анализ материалов уголовного дела, оперативных данных и другой имеющейся информации. Классификация мер предупреждения компьютерных преступлений. Правовые меры предупреждения. Меры предупреждения организационно-технического характера. Криминалистические меры предупреждения. Организационные мероприятия по предупреждению криминалистических преступлений. Методы регистрации попыток НСД.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление проектами в области информационной безопасности

Электронные ресурсы (издания)

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

1. *Московское отделение Института управления проектами - Project Management Institute PMI – www.pmi.ru*
2. *Национальная ассоциация управление проектами «СОВНЕТ» (корпоративный член международной организации управления проектами IPMA) – www.sovnet.ru*
3. *Технологии корпоративного управления. Проектное управление. – http://www.iteam.ru/publications/project/*

Печатные издания

1. Кэрриэ Б. Криминалистический анализ файловых систем: Пер. с англ. / Б. Кэрриэ. – СПб.: Питер, 2007. – 479 с.

2. Журавленко, Н.И. Информационная безопасность и защита от информационного воздействия: учебное пособие: учеб. пособие / Н.И. Журавленко, А.С. Овчинский. — Электрон. дан. — Уфа: БГПУ имени М. Акмуллы, 2010. — 168 с.

3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМКПресс, 2010. -544 с.

4. Джеймс Л. Фишинг. Техника компьютерных преступлений / Лэнс Джеймс ; [пер. с англ. Р. В.Гадицкого] .— Москва : НТ Пресс, 2008 .— 314 с.

5. Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонсторх; Пер. с англ. В.И. Воропаева, Г.Г. Трехалина .— М. : Мир, 1999 .— 352 с.

6. Брэгг Р. Безопасность сетей. Полное руководство / Роберта Брэгг, Марк Родс-Оусли, Кит Страссберг ; [пер. с англ. Т. Трубникова, Я. Майсовой, М. Фадеевой] .— Москва : ЭКОМ : БИНОМ. Лаборатория знаний, 2006. — 912 с

7. Белкин, П. Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов / П.Ю. Белкин, О.О. Михальский, А.С.Першаков и др. — М.: Радио и связь, 2000.— 168 с.

8. Просис, К. Расследование компьютерных преступлений / К. Просис, К. Мандиа ; пер. с англ. О.Труфанова ; науч. ред. А. Головко .— Москва : Лори, 2013 .— 476 с.

9. Копылов, В. А. Информационное право : Учебник / В. А. Копылов ; Моск. гос. юрид. акад. — 2-е изд., перераб. и доп. — Москва : Юристъ, 2002 .— 512 с

5.1.2. Дополнительная литература

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.

2. Право и информационная безопасность: [учеб. пособие] / А. П. Фисун, А. Н. Касилов, Ю. А.Глоба [и др.]; [под ред. А. П. Фисуна и Ю. А. Белевской]; Орл. юрид. ин-т МВД России, Орл.регион. акад. Гос. службы, Орл. гос. ун-т.— Москва: Приор-издат, 2005 .— 272 с

3. Ковалев А. А. Информационная политика и военная безопасность России в эпоху противостояния цивилизаций: теоретико-методологические аспекты проблемы: монография / А.А. Ковалев. — Санкт-Петербург, 2016 .— 193 с

4. Леонтьев, Б. Хакеры, взломщики и другие информационные убийцы.— М. : Познавательная книга плюс,1999 .— 192 с.

5. Федотова, Е. Л. Информационные технологии и системы: учебное пособие для студентов вузов, обучающихся по специальности 080801 "Прикладная математика" и другим техническим специальностям / Е. Л. Федотова.— Москва : ФОРУМ : ИНФРА-М, 2014 .— 352 с.

6. Губенков, А. А. Информационная безопасность : [учеб. пособие] / А. А. Губенков, В. Б.Байбурин .— Москва : Новый издательский дом, 2005 .— 128 с.

7. Макнамара Д. Секреты компьютерного шпионажа: Тактика и контрмеры/Пер. с англ.; Под ред.

С.М.Молявко –М.: БИНОМ. Лаборатория знаний,2004. -536 с.

8. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.:Наука и Техника, 2004. – 384 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

[*список с указанием наименования баз данных, информационно-справочных и поисковых систем*]

www.consultant.ru. - www.garant.ru. - Электронно- библиотечная **система** ZNANIUM.COM – режим доступа www.znanium.com.

- Научная электронная библиотека eLIBRARY.RU – режим доступа http://elibrary.ru.
- Электронная библиотека Grebennikon – режим доступа http://grebennikon.ru/.
- Универсальная справочно-информационная полнотекстовая **база данных** периодических изданий EastViewhttp://ebiblioteka.ru/.

2.4. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 2

Управление проектами в области информационной безопасности

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
	Лекции; Лабораторные занятия; Консультации; Самостоятельная работа студентов;	*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*	• *Компьютер, на котором установлено программное обеспечение: MS Excel, Project Expert 7, MS Project.*