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
«_27_» апреля 2021 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля
1156875

Модуль
Методы и системы обнаружения компьютерных атак

Екатеринбург, 2021

1.

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

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

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Методы и средства обнаружения компьютерных атак

1.1. Аннотация содержания модуля

Рассматриваются основные этапы применения систем обнаружения атак разработке и эксплуатации. Изучаются понятия сетевых компьютерных атак. Проводится анализ основных типов систем обнаружения атак, применяемых на практике в настоящее время, описаны математические модели, используемые в качестве базы для алгоритма обнаружения компьютерных атак.

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.	Аппаратные средства вычислительной техники	*4/144*
2	Методы и средства противодействия вредоносному программному обеспечению	*4/144*
	Методы обнаружения и противодействия компьютерным атакам	*3/108*
	ИТОГО по модулю:	*11/396*

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Информационные технологии Компьютерное моделирование Основы технической защиты информации
Постреквизиты и корреквизиты модуля	Управление информационной безопасностью Защита информации Технические средства и методы защиты информации Физическая культура и спорт

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*** *)*
ОПК-13. Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности	"РО1-З ОПК12 Знает классификацию систем основные законы и закономерности систем"	"РО1-УОПК12 Умеет выделять систему из внешней среды; выполнять декомпозицию системы"	"РО1-В ОПК12 Владеет методиками системного анализа"	

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной форме

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

ПРОГРАММА МОДУЛЯ

Методы и средства обнаружения компьютерных атак

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1

Аппаратные средства вычислительной техники

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	*Учебно-научный центр «Информационная безопасность»*

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 1

Аппаратные средства вычислительной техники

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	Схемотехника электронных цифровых устройств	Базовые схемы логических элементов (ЛЭ). Триггеры. Регистры памяти и сдвига. Счетчики импульсов. Комбинационные логические элементы в составе серий ИС. Формирователи импульсов. Мультивибраторы
2	Микропроцессоры в телекоммуникационных системах	Микропроцессоры как новая технологическая база построения различных устройств телекоммуникационных систем. Основные понятия, виды архитектур, типы микропроцессоров. Состояние, перспективы и тенденции развития универсальных и специализированных микропроцессоров и их использование для построения элементов сетей передачи данных.
3	Коммуникационные микропроцессоры	Классификация, показатели и архитектура коммуникационных микропроцессоров. Память, параллельные порты ввода/вывода и протоколы последовательного обмена. АЦП, ЦАП, таймеры и процессоры событий. Современные коммуникационные микропроцессоры и их использование в оборудовании сетей связи.
4	Сигнальные микропроцессоры	Классификация, характеристики и архитектура цифровых сигнальных микропроцессоров. Память и арифметические узлы. Система команд. Состав команд арифметических и логических операций, операций передачи данных, управления и вызова подпрограмм. Способы адресации. Средства программирования отладки программ. Программная модель сигнального микропроцессора. Типы современных цифровых сигнальных микропроцессоров и их использование в оборудовании сетей связи.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Аппаратные средства вычислительной техники

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. Хартов, В. Я. Микропроцессорные системы: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" / В. Я. Хартов.— 2-е изд., испр. и доп. — Москва: Академия, 2014.

2. Калашников В. И. Электроника и микропроцессорная техника: учебник для студентов вузов, обучающихся по направлению подготовки бакалавров "Приборостроение" / В. И. Калашников, С. В. Нефедов ; под ред. Г. Г. Раннева .— Москва: Академия, 2012.

3. Зиатдинов, С. И. Схемотехника телекоммуникационных устройств: учебник для студентов [вузов], обучающихся по направлению подготовки 210700 "Инфокоммуникационные технологии и системы связи" / С. И. Зиатдинов, Т. А. Суетина, Н. В. Поваренкин .— Москва : Академия, 2013.

4. Гусев, В. Г. Электроника и микропроцессорная техника : учебник для вузов / В. Г. Гусев, Ю. М. Гусев .— 4-е изд., доп. — М.: Высшая школа, 2006 – 621 с.

5. Таненбаум, Э. Распределенные системы. Принципы и парадигмы / Э. Таненбаум, М. ван Стеен ; [пер. с англ. В. Горбункова].— М.; СПб.; Нижний Новгород: Питер, 2003. — 877 с.

6. Безуглов, Д. А. Цифровые устройства и микропроцессоры : учеб. пособие для вузов / Д. А. Безуглов, И. В. Калиенко .— Ростов-на-Дону: Феникс, 2006 – 528 с.

7. Нарышкин, А. К. Цифровые устройства и микропроцессоры : учебное пособие для студ. вузов радиотехн. специальностей / А. К. Нарышкин .— 2-е изд., стер. — М.: Академия, 2008.

8. Семенов, Ю. А. Алгоритмы телекоммуникационных сетей : учебное пособие [для вузов] / Ю. А. Семенов .— М. : Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2007.

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

Не требуются.

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 и средства обнаружения компьютерных атак

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 2

Методы и средства противодействия вредоносному программному обеспечению

Рабочая программа дисциплины составлена авторами:

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

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 2

Методы и средства противодействия вредоносному программному обеспечению

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	Информационные и компьютерные преступления	Понятие об информационных и компьютерных преступлениях. Особенности и причины информационных преступлений. 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. Особенности подготовки компьютерных преступлений.
2	Понятие об опасной компьютерной информации	Создание и использование компьютерных программ как деятельность, представляющая повышенную общественную опасность. Уровни представления опасной компьютерной информации. Понятие компьютерных программ и команд. Программы и данные как объективная форма представления компьютерной информации. Машинный код. Ассемблерные команды. Опасные системные вызовы. Опасные системные команды. Инструментарий для разработки, отладки и модификации вредоносных программ.
3	Классификация и технические возможности вредоносных программ	Понятие о вредоносных программах. Классификация вредоносных программ по основным свойствам и признакам. Классификация программ по степени опасности для защищаемой информации и компьютерной системы. Деструктивные функции вредоносных программ. Механизмы вирусного заражения. Способы выявления деструктивной активности программ. Понятие о сигнатуре вредоносного программного кода. Принцип антивирусного сканирования. Антивирусные сканеры, мониторы и сетевые фильтры.
4	Уязвимые места программного обеспечения ЭВМ, способствующие внедрению, сокрытию, распространению и запуску вредоносных программ.	Потенциально опасные функции и элементы операционной системы. Возможности использования уязвимостей ОС и штатного программного обеспечения с целью удаления, модификации, блокирования или копирования информации без уведомления и согласия ее владельца или пользователя. Защита компьютерных систем от вредоносного программного воздействия. Понятие об опасных и вредоносных программах. Характеристика компьютерной программы как вида информационного нарушителя. Классификация вредоносных программ. Демаскирующие признаки опасного программного

		воздействия. Основные организационные и программные меры антивирусной защиты.
5	Изучение функциональных возможностей вредоносных программ	Основные признаки и возможности макровирусов, сетевых «червей», программ «удаленного администрирования». Способы проникновения вредоносных программ в локальные и сетевые ЭВМ. Способы выявления деструктивной активности вредоносных программ. Понятие о сигнатуре вредоносного программного кода. Принцип антивирусного сканирования. Понятие о механизмах скрытности вредоносных программ. Демаскирующие признаки вредоносного программного кода. Полиморфизм программного кода. Программы-«невидимки». Способы сокрытия файловых объектов и процессов на уровне ядра операционной системы. Возможности программ-«руткитов».

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 Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Пер. с англ. / Дэвид Айков, Карл Сейгер, Уильям Фонсторх. – М.: Мир, 1999. – 351 с.

2. Бакланов В.В. Опасная компьютерная информация / В.В.Бакланов. Екатеринбург, в/ч 69617. 2006. 123 с.

3. Вехов В. Б. Тактические особенности расследования преступлений в сфере компьютерной информации: научно-практ. пособие – 2-е изд., доп. и испр. / В. Б. Вехов, В. В. Попова, Д. А. Илюшин. – М.: ЛексЭст, 2004. – 160 с.

4. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А. Г. Волеводз. – М.: ООО Издательство Юрлитинформ, 2002. – 496 с.

5. Гаврилин Ю. В. Преступления в сфере компьютерной информации: квалификация и доказывание : учеб. пособие / Ю. В. Гаврилин, А. В. Кузнецов, А. Ю. Головин, Т. В. Толстухина, А. В. Кузнецов. – М.: ЮИ МВД РФ, 2003. – 245 с.

6. Кэрриэ Б. Криминалистический анализ файловых систем: Пер. с англ. / Б. Кэрриэ. – СПб.: Питер, 2007. – 480 с.

7. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью / В. Е. Козлов. – М.: Горячая линия – Телеком, 2002. – 336 с.

8. Мазуров В. А. Компьютерные преступления: классификация и способы

противодействия: учеб. – практическое пособие / В. А. Мазуров. – М.: Палеонтип, Логос, 2002. – 148 с.

9. Макнамара Д. Секреты компьютерного шпионажа: Тактика и контрмеры Пер. с англ. / Д. Макнамара. – М.: БИНОМ. Лаборатория знаний, 2004. – 536 с.

10. Мандиа К. Защита от вторжений. Расследование компьютерных преступлений: Пер. с англ. / К. Мандиа, К. Просис. – М.: ЛОРИ, 2005. – 476 с.

11. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография / А. Л. Осипенко. – М.: Норма, 2004. – 432 с.

12.Соловьев Л. Н. Вредоносные программы: расследование и предупреждение преступлений / Л. Н. Соловьев. – М.: Собрание, 2004. – 224 с.

13. Усов А. И. Судебно-экспертное исследование компьютерных средств и систем: Основы методического обеспечения: учеб. пособие / А. И. Усов. – М.: Изд-во Экзамен, Право и закон, 2003. – 368 с.

14.Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. – М.: СК Пресс, 1998. – 288 с., ил.

15.Касперский К. Техника и философия хакерских атак. - М.: «Солон - Р», 1999, 272с.

16.Крис Касперски. Укрощение Интернета. –М.: СОЛОН-Р, 2002. –288 с.

17.Скэмбрей Джоел, Мак-Клар Стюарт. Секреты хакеров. Безопасность Windows 2000 – готовые решения. Пер. с англ. –М.: Издательский дом «Вильямс», 2002. –464 с.

18.Стюарт Мак-Клар, Джоел Скембрей, Джордж Курц. Секреты хакеров. Безопасность сетей - готовые решения, 2-е изд.: Пер. с англ. - М.: Издательский дом "Вильямс", 2001. -656 с.

5.1.2. Дополнительная литература

1. Крылов В. В. Информационные компьютерные преступления / В. В. Крылов. – М.: ИНФРА-М-НОРМА, 1997. – 285 с.

2. Курушин В. Д. Компьютерные преступления и информационная безопасность: справочник / В. Д. Курушин, В. А. Минаев. – М.: Новый Юрист, 1998. – 256 с.

3. Леонтьев Б. Хакеры, взломщики и другие информационные убийцы / Б. Леонтьев. – М.: Познавательная книга, 1999. – 192 с.

4. Медведовский И. Д. Атака на Internet: – 2-е изд., перераб. И доп. / И. Д. Медведовский, П. В. Семьянов, Д. Г. Леонов. – М.: ДМК, 1999. – 336 с.

5. Гульев И. Компьютерные вирусы, взгляд изнутри — М.: ДМК, 1998 — 304 с.

6. Таненбаум Э. Современные операционные системы. 2-е изд. -СПб.: Питер, 2002. - 1040 с.

7. Хоникатт Джерри. Реестр Windows 2000. Пер. с англ. Уч. пос. –М.: Издательский дом «Вильямс», 2000. –320 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

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.*

ПРОГРАММА МОДУЛЯ

Методы и средства обнаружения компьютерных атак

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 3

Методы обнаружения и противодействия компьютерным атакам

Рабочая программа дисциплины составлена авторами:

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

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

3. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 3

Методы обнаружения и противодействия компьютерным атакам

3.1. 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);*

3.2. Содержание дисциплины

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Основы компьютерных сетей	Введение в основы компьютерных сетей. Основные протоколы прикладного уровня стека TCP/IP. Основные протоколы транспортного, сетевого и канального уровня стека TCP/IP. Сетевое оборудование, принципы работы. Vlan и Vpn, принципы построения сетей. Передача пакетов на сетевом и канальном уровнях.
2	Мониторинг событий информационной безопасности	Виды систем защиты информации. Принципы работы и использования систем защиты информации: Host IDS, Network IDS/IPS, Antivirus, Data Loss Prevention, Web Application Firewall, Proxy, Firewall, Vulnerability Scanner, Sandbox, SIEM. Принципы выявления атак на основе модели Cyber-Kill Chain. События ИБ и их анализ для выявления атак. Инциденты ИБ. Способы реагирования на инциденты ИБ.
3	Технические средства обнаружения вторжений	Архитектура и общее описание стека технологий ELK. Изучение агентов для сбора информации с ОС Windows, Linux. Логирование ОС Windows, политики аудита. Изучение возможностей Sysmon. Изучение возможностей системы Network IDS Suricata. Принципы работы с консолью Kibana для поиска и анализа событий ИБ. Разработка запросов на языке Query DSL. Изучение принципов разработки панелей визуализации событий. Изучение общих принципов разворачивания инструментов для мониторинга и диагностики неисправностей.
4	Методы автоматизации выявления инцидентов ИБ.	Изучение принципов автоматизации выявления инцидентов ИБ, применяемых в SIEM системах. Разработка правил автоматизированного выявления на примере подсистемы «Сигнал».

3.3. 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. "Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация", Уэндел Од.

2. Внутреннее устройство Windows , Марк Руссинович, Дэвид Соломон, Алекс Ионеску, Павел Йосифович.

3. "Windows Internals: Covering Windows Server 2008 R2 and Windows 7 Марк Руссинович, Дэвид Соломон, Алекс Ионеску.

4. MITRE ATT&CK (attack.mitre.org)

Внутреннее устройство Linux - Брайан Уорд

5. "Нормативная база и стандарты в области информационной безопасности", Ю. Родичев

6. "Информационная безопасность: защита и нападение", А. Бирюков.

7. "Лаборатория хакера", С. А. Бабин

Печатные издания

1 Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Пер. с англ. / Дэвид Айков, Карл Сейгер, Уильям Фонсторх. – М.: Мир, 1999. – 351 с.

2. Бакланов В.В. Опасная компьютерная информация / В.В.Бакланов. Екатеринбург, в/ч 69617. 2006. 123 с.

3. Вехов В. Б. Тактические особенности расследования преступлений в сфере компьютерной информации: научно-практ. пособие – 2-е изд., доп. и испр. / В. Б. Вехов, В. В. Попова, Д. А. Илюшин. – М.: ЛексЭст, 2004. – 160 с.

4. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А. Г. Волеводз. – М.: ООО Издательство Юрлитинформ, 2002. – 496 с.

5. Гаврилин Ю. В. Преступления в сфере компьютерной информации: квалификация и доказывание : учеб. пособие / Ю. В. Гаврилин, А. В. Кузнецов, А. Ю. Головин, Т. В. Толстухина, А. В. Кузнецов. – М.: ЮИ МВД РФ, 2003. – 245 с.

6. Кэрриэ Б. Криминалистический анализ файловых систем: Пер. с англ. / Б. Кэрриэ. – СПб.: Питер, 2007. – 480 с.

7. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью / В. Е. Козлов. – М.: Горячая линия – Телеком, 2002. – 336 с.

8. Мазуров В. А. Компьютерные преступления: классификация и способы противодействия: учеб. – практическое пособие / В. А. Мазуров. – М.: Палеонтип, Логос, 2002. – 148 с.

9. Макнамара Д. Секреты компьютерного шпионажа: Тактика и контрмеры Пер. с англ. / Д. Макнамара. – М.: БИНОМ. Лаборатория знаний, 2004. – 536 с.

10. Мандиа К. Защита от вторжений. Расследование компьютерных преступлений: Пер. с англ. / К. Мандиа, К. Просис. – М.: ЛОРИ, 2005. – 476 с.

11. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография / А. Л. Осипенко. – М.: Норма, 2004. – 432 с.

12.Соловьев Л. Н. Вредоносные программы: расследование и предупреждение преступлений / Л. Н. Соловьев. – М.: Собрание, 2004. – 224 с.

13. Усов А. И. Судебно-экспертное исследование компьютерных средств и систем: Основы методического обеспечения: учеб. пособие / А. И. Усов. – М.: Изд-во Экзамен, Право и закон, 2003. – 368 с.

14.Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. – М.: СК Пресс, 1998. – 288 с., ил.

15.Касперский К. Техника и философия хакерских атак. - М.: «Солон - Р», 1999, 272с.

16.Крис Касперски. Укрощение Интернета. –М.: СОЛОН-Р, 2002. –288 с.

17.Скэмбрей Джоел, Мак-Клар Стюарт. Секреты хакеров. Безопасность Windows 2000 – готовые решения. Пер. с англ. –М.: Издательский дом «Вильямс», 2002. –464 с.

18.Стюарт Мак-Клар, Джоел Скембрей, Джордж Курц. Секреты хакеров.

Безопасность сетей - готовые решения, 2-е изд.: Пер. с англ. - М.: Издательский дом "Вильямс", 2001. -656 с.

5.1.2. Дополнительная литература

1. Крылов В. В. Информационные компьютерные преступления / В. В. Крылов. – М.: ИНФРА-М-НОРМА, 1997. – 285 с.

2. Курушин В. Д. Компьютерные преступления и информационная безопасность: справочник / В. Д. Курушин, В. А. Минаев. – М.: Новый Юрист, 1998. – 256 с.

3. Леонтьев Б. Хакеры, взломщики и другие информационные убийцы / Б. Леонтьев. – М.: Познавательная книга, 1999. – 192 с.

4. Медведовский И. Д. Атака на Internet: – 2-е изд., перераб. И доп. / И. Д. Медведовский, П. В. Семьянов, Д. Г. Леонов. – М.: ДМК, 1999. – 336 с.

5. Гульев И. Компьютерные вирусы, взгляд изнутри — М.: ДМК, 1998 — 304 с.

6. Таненбаум Э. Современные операционные системы. 2-е изд. -СПб.: Питер, 2002. - 1040 с.

7. Хоникатт Джерри. Реестр Windows 2000. Пер. с англ. Уч. пос. –М.: Издательский дом «Вильямс», 2000. –320 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

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/.

3.5 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*	• *Компьютер, на котором установлено программное обеспечение: MS Excel, Project Expert 7, MS Project.*

		обеспечение, средства защиты информации	