МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт физики

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский
_____ «___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем

Направление подготовки: 10.04.01 - Информационная безопасность
Профиль подготовки: Информационная безопасность автоматизированных систем
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

Содержание

Программу дисциплины разработал(а)(и) младший научный сотрудник, б/с Лапшина И.Р. (НИЛ СВЧ проектирование и радиотелекоммуникации, Институт физики), IRTuktarova@kpfu.ru ; Иванов Константин Васильевич

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-2	способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения
ПК-1	способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты
ПК-10	способностью проводить аттестацию объектов информатизации по требованиям безопасности информации
ПК-2	способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности
ПК-3	способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов
ПК-4	способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности
ПК-7	способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента
ПК-8	способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи
ПК-9	способностью проводить аудит информационной безопасности информационных систем и объектов информатизации

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- понятие, структуру, функции и области применения экспертных систем комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем;
- основные тенденции развития экспертных систем;
- программные и технические средства разработки, технологию создания экспертных систем;
- методы сбора и анализа информации, поиска решений в экспертных системах;
- основные технические характеристики и принципы работы современных экспертных систем комплексной оценки безопасности.

Должен уметь:

- выбирать формальную модель представления полученных данных;
- выбирать программно-технические средства для разработки экспертных систем;
- использовать современные подходы в области защиты информации, в том числе новейший математический аппарат по решению задач информационной безопасности;
- использовать современные информационные технологии для изучения экспертных систем комплексной оценки информационной безопасности.

Должен владеть:

- навыками классификации данных, предназначенных для обработки экспертными системами;
- методами поиска решения в экспертных системах;
- навыками проектирования экспертных систем;
- навыками эксплуатации современных экспертных систем комплексной оценки безопасности.

Должен демонстрировать способность и готовность:

- проводить классификацию и анализ данных, обрабатываемых экспертными системами комплексной оценки информационной безопасности;
- применять существующие экспертные системы комплексной оценки для решения задач по обеспечению безопасности автоматизированных систем;
- разрабатывать методику работы и проектировать архитектуру экспертных систем;
- создавать программно-аппаратное обеспечение для экспертных систем комплексной оценки информационной безопасности.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ОД.12 Дисциплины (модули)" основной профессиональной образовательной программы 10.04.01 "Информационная безопасность (Информационная безопасность автоматизированных систем)" и относится к обязательным дисциплинам.
Осваивается на 2 курсе в 3 семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) на 108 часа(ов).

Контактная работа - 28 часа(ов), в том числе лекции - 10 часа(ов), практические занятия - 18 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 44 часа(ов).

Контроль (зачёт / экзамен) - 36 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 3 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Общая теория экспертных систем комплексной оценки информационной безопасности	3	2	2	0	8
2.	Тема 2. Данные для анализа в экспертных системах. Типы, классификация, сбор и подготовка данных.	3	2	4	0	8
3.	Тема 3. Программные и аппаратные средства экспертных систем комплексной оценки информационной безопасности	3	2	4	0	10
4.	Тема 4. Методы проектирования экспертных систем комплексной оценки ИБ	3	2	4	0	10
5.	Тема 5. Современные экспертные системы комплексной оценки ИБ	3	2	4	0	8
	Итого		10	18	0	44

4.2 Содержание дисциплины (модуля)

Тема 1. Общая теория экспертных систем комплексной оценки информационной безопасности

Понятие и структура автоматизированной экспертной системы. Принципы оценки информационной безопасности автоматизированных информационных и телекоммуникационных систем. Структура и функции экспертной системы комплексной оценки информационной безопасности. Классификация экспертных систем оценки ИБ.

Тема 2. Данные для анализа в экспертных системах. Типы, классификация, сбор и подготовка данных.

Особенности и основные отличительные признаки необходимых данных об исследуемой автоматизированной системе. Типы данных, их представление в разных подсистемах экспертной системы. Классы данных. Методы сбора и подготовки данных для обработки в экспертной системе. Методы анализа данных.

Тема 3. Программные и аппаратные средства экспертных систем комплексной оценки информационной безопасности

Программные средства экспертных систем: процедуры и программы сбора данных о подсистеме защиты информации автоматизированной системы, функции-обработчики данных, базы данных, элементы искусственного интеллекта для анализа полученных данных и синтеза решений. Аппаратные средства экспертных систем: средства сбора информации, средства обработки информации.

Тема 4. Методы проектирования экспертных систем комплексной оценки ИБ

Основные подсистемы экспертной системы комплексной оценки ИБ. Подходы к проектированию экспертных систем. Особенности проектирования систем комплексной оценки ИБ. Общая методика проектирования экспертных систем оценки ИБ. Особенности тестирования автоматизированных систем при помощи экспертных систем оценки ИБ, достоверность оценки ИБ.

Тема 5. Современные экспертные системы комплексной оценки ИБ

Системы комплексного аудита информационной безопасности автоматизированных систем. Сканеры информационной безопасности. Экспертные системы оценки информационной безопасности автоматизированных систем на основе искусственного интеллекта.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301)

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);
- критерии оценивания сформированности компетенций;
- механизм формирования оценки по дисциплине (модулю);
- описание порядка применения и процедуры оценивания для каждого оценочного средства;
- критерии оценивания для каждого оценочного средства;
- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;

- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Официальная страница сканера безопасности MaxPatrol - https://www.ptsecurity.com/ru-ru/products/mp8/

Официальная страница сканера безопасности XSpider - https://www.ptsecurity.com/ru-ru/products/xspider/

Официальный сайт сканера безопасности Nessus - http://www.tenable.com/

9. Методические указания для обучающихся по освоению дисциплины (модуля)

На самостоятельную работу отводится 44 академических часа. В ходе самостоятельной работы магистрант готовится к устному опросу по темам 1 и 2.

Для подготовки используется лекционный материал, а также материал из рекомендуемой и дополнительной литературы. Магистрант готовится по группе вопросов,

выносимых на обсуждение на практическое занятие по теме, которые предлагаются преподавателем по окончанию каждого лекционного занятия.

Устный опрос предполагает проверку усвоения магистрантами пройденного материала. Также не исключается дискуссия между магистрантом и преподавателем

по наиболее важным и спорным вопросам дисциплины с целью проверки понимания материала.

Письменная работа по материалу темы 3 представляет собой развернутый и обоснованный письменный ответ на вопрос о необходимом перечне программных и/или аппаратных средств для создания экспертной системы комплексной оценки информационной безопасности предложенной преподавателем автоматизированной информационной или телекоммуникационной системы. Для успешного выполнения необходимо повторить материал лекций 1-3, а также воспользоваться литературой и интернет-ресурсами, рекомендованными преподавателем.

Презентация на основе материала темы 4 представляет собой развернутое решение поставленной магистрантам практической задачи по созданию модели и проектированию архитектуры экспертной системы оценки ИБ выбранной автоматизированной информационной или телекоммуникационной системы. Для подготовки презентации используются материалы лекций 1-4, результаты письменной работы по теме 3, а также литература и интернет-ресурсы, рекомендованные преподавателем. В целях облегчения проектирования экспертной системы решения преподаватель после освоения темы 4 выдает магистрантам рекомендации по подготовке к презентации.

Проверка практических навыков магистрантов предусматривает выполнение индивидуальных работ по оценке защищенности ОС семейства Linux и Window при помощи инструментария сканеров безопасности. По итогам работы составляется отчет по аудиту указанных систем с интерпретацией результатов.

Подготовка к экзамену по осваиваемой дисциплине ведется по установленному списку вопросов, выдаваемому магистрантам преподавателем не позже чем за две недели

до даты сдачи экзамена. Каждый магистрант получает на экзамене билет с двумя вопросами по пройденному материалу и готовит на них письменный ответ в течение 40

минут. Сдача экзамена происходит в устной форме, в случае необходимости преподаватель имеет право задавать дополнительные вопросы на любую пройденную

тему дисциплины.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Мультимедийная аудитория.

Компьютерный класс.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 10.04.01 "Информационная безопасность" и магистерской программе "Информационная безопасность автоматизированных систем".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ОД.12 Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль подготовки: Информационная безопасность автоматизированных систем

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2017

Основная литература:

1. Жук А. П. Защита информации [Электронный ресурс]: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование:Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6, 500 экз. http://znanium.com/bookread.php?book=474838

2. Поддержка принятия решений при проектировании систем защиты информации: Монография / В.В. Бухтояров, В.Г. Жуков, В.В. Золотарев. - М.: НИЦ ИНФРА-М, 2014. - 131 с.: 60x88 1/16. - (Научная мысль; Информатика). (о) ISBN 978-5-16-009516-6, 150 экз. Режим доступа: http://znanium.com/bookread2.php?book=445551

3. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с.: 60x90 1/16. - (Профессиональное образование) (Обложка) ISBN 978-5-00091-079-5, 300 экз.

http://znanium.com/bookread2.php?book=508381

Дополнительная литература:

1. Аверченков, В. И. Аудит информационной безопасности [электронный ресурс] : учеб.пособие для вузов / В. И. Аверченков. - 2-е изд., стереотип. - М. : Флинта, 2011. - 269 с. - ISBN 978-5-9765-1256-6

http://znanium.com/bookread2.php?book=453734

2. Аверченков, В. И. Служба защиты информации : организация и управление [электронный ресурс] : учеб. пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 2-е изд., стереотип. - М. : ФЛИНТА, 2011. - 186 с. - ISBN 978-5-9765-1271-9. Режим доступа: http://znanium.com/bookread2.php?book=453915

3. Основы управления информационной безопасностью. Серия 'Вопросы управление информационной безопасностью'. Выпуск 1 [Электронный ресурс] : учеб. пособие / А.П. Курило [и др.]. ? Электрон. дан. ? Москва : Горячая линия-Телеком, 2012. ? 244 с. ? Режим доступа: https://e.lanbook.com/book/5178

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ОД.12 Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем

Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль подготовки: Информационная безопасность автоматизированных систем

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2017

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.