МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 г.

Рабочая программа дисциплины
Техническое противодействие компьютерной разведке

Направление подготовки (специальности)
10.03.01 Информационная безопасность

Направленность (профиль)
«Безопасность компьютерных систем»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целями освоения дисциплины «Техническое противодействие компьютерной разведке» являются теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий выявления и противодействия формам и методам ведения компьютерной разведки.

Данный курс, на основеиспользования международных российских стандартов и нормативных требований в сфере управления информационной безопасностью, вырабатывает у студентов знания и навыки применения аппаратного и программного обеспечения для технического противодействия компьютерной разведке, применяемой против российских объектов информатизации.

2. Место дисциплины в структуре ОП

«Техническое противодействие компьютерной разведке»относится к числу дисциплин базовой части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владелзнаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» – работа с программными средствами общего назначения;

«Аппаратные средства вычислительной техники» – знание архитектуры основных типов современных компьютерных систем;

«Операционные системы» – знание принципов построения современных операционных систем и особенностей их применения, владение навыками конфигурирования и администрирования операционных систем;

«Защита программ и данных» - умение применять средства обнаружения вторжений иантивирусной защиты;

«Защита в операционных системах» – умение формулировать и настраивать политику безопасности для основных операционных систем.

Знания и навыки, полученные в результате изучении дисциплины «Техническое противодействие компьютерной разведке», используются студентами при разработке курсовых и дипломных работ.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО 2016 года для специальности КБ, направленных на приобретение следующих знаний, умений, навыков и (или) опыта деятельности:

Код компетенции	Формулировка компетенции	Перечень планируемых результатов обучения
Профессиональные компетенции		
ПК-12	способность проводить инструментальный мониторинг защищенности компьютерных систем.	**Знать:** – методы проведения инструментального мониторинга защищенности компьютерных систем. **Уметь:** –применять специальные методы и средства для инструментального мониторинга защищенности компьютерных систем. **Владеть навыками:** – проведения инструментального мониторинга защищенности компьютерных систем.

ПК-19	способность проводить проверки технического состояния и профилактические осмотры технических средств защиты информации.	**Знать:** – формы проведения проверки технического состояния средств защиты информации; -методы и способы проведения профилактических осмотров технических средств защиты информации. **Уметь** проводить проверки технического состояния и профилактические осмотры технических средств защиты информации. **Владеть навыками** проведения проверок технического состояния и профилактических осмотров технических средств защиты информации.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	Самостоятельная работа	
1	Цели и задачи компьютерной разведки, формы и условия ее проведения. Роль, место и формы противодействия компьютерной разведке.	9	4	2				7	Задания для самостоятельной работы
2	Методы выявления признаков и фактов проведения компьютерной разведки.	9	4	2		1		7	Задания для самостоятельной работы
3	Оценка уязвимости систем для компьютерной разведки.	9	4	4		1		7	Задания для самостоятельной работы
4	Средства и методы обнаружения вторжений в информационные системы.	9	4	2		1		7	Задания для самостоятельной работы
5	Противодействие программным закладкам.	9	4	4		1		7	Задания для самостоятельной работы
6	Комплекс мер технического противодействия компьютерной разведке.	9	8	2				6	
7	Методы управления информационной безопасностью.	9	8	2				8	
						1	3		Зачет
	Всего за 9 семестр		36	18		5	3	49	
	Всего		**36**	**18**		**5**	**3**	**49**	

Содержание разделов дисциплины:

Тема 1. Цели и задачи компьютерной разведки, формы и условия ее проведения. Роль, место и формы противодействия компьютерной разведке.

1.1. Цели, задачи и особенности (в смысле условия) проведения компьютерной конкурентной разведки, использования методов компьютерной разведки в меркантильных противоправных целях, а также в противоправных политических целях, для реализации идеологии терроризма и экстремизма.

1.2. Роль, место и формы организационно-юридического и технического противодействия методам компьютерной разведки объектов российской информационной инфраструктуры.

Тема 2. Методы выявления признаков и фактов проведения компьютерной разведки.

2.1. Использование штатных общедоступных иностранных и специальных российских технологий мониторинга (как в части аудита, и применении самостоятельных инструментальных средств) для выявления признаков и фактов проведения компьютерной разведки в широкополосных сетях, сетях общего доступа, современных беспроводных сетях связи, на отдельных критически важных объектах информационной инфраструктуры.

2.2.Проверка устройств на возможное наличие закладных аппаратных или программных средств компьютерной разведки. Руководящий документ гостехкомиссии России (ФСТЭК России) от 04.06.1999г. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

Тема 3. Оценка уязвимости систем для компьютерной разведки.

3.1. Методы выявления уязвимости объектов информатизации для средств проведения компьютерной разведки.

3.2. Оценка эффективности принимаемых защитных мер. Обзор семейства национальных стандартов ГОСТ Р ИСО/МЭК 53113-1-2008, ГОСТ Р ИСО/МЭК 53113-2-2009, ГОСТ Р ИСО/МЭК 56545-2015, ГОСТ Р ИСО/МЭК 56546-2015.

3.3. Дополнительное изучение истории и содержания инцидентов безопасности. Обзор банка данных угроз безопасности ФСТЭК России.

Тема 4. Средства и методы обнаружения атак и вторжений в информационные системы.

4.1. Выявление и отражение компьютерных атак. Законодательство России в сфере защиты критических информационных систем (Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ)

4.2. Антихакинг как система выявления признаков злонамеренного изучения открытых сервисов и защитных механизмов системы.

4.3. Системы обнаружения вторжений. Обзор профилей защиты по системам 4, 5 и 6 классов из нормативных документов ФСТЭК России, введенных приказом ФСТЭК России от 6 декабря 2011 г. № 638 (зарегистрирован Минюстом России 1 февраля 2012 г., рег. №23088) утверждены «Требования к системам обнаружения вторжений», которые вступили в действие с 15 марта 2012г.

Тема 5. Противодействие программным закладкам.

5.1. Формы и методы противодействия программным закладкам.

5.2. Антивирусные средства. Обзор требований по антивирусной защите для ИС 4, 5 и 6 классов из нормативных документов ФСТЭК России, введенных приказом ФСТЭК России от 20 марта 2012 г. № 28 «Требования к средствам антивирусной защиты».

5.3. Системы-ловушки.

Тема 6. Комплекс мер технического противодействия компьютерной разведке.

6.1. Разработка вариантов совершенствования имеющихся мер технического противодействия компьютерной разведке на российских объектах информатизации.

6.2. Современные и перспективные российские аппаратные, программные и аппаратно-программные комплексы технического противодействия компьютерной разведке, их назначение и функциональные возможности. Обзор типовых аппаратно-программных решений российских компаний.

Тема 7. Методы управления информационной безопасностью.

7.1.Управление информационной безопасностью как универсальное средство технического противодействия компьютерной разведке.

7.2. Международные российские стандарты управления безопасностью. Методики реализации средств технического противодействия компьютерной разведке.

7.3. Разработка, внедрение и поддержание адекватной политики информационной и компьютерной безопасности на защищаемых российских объектах информатизации, контроль за ее эффективностью и меры совершенствования.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

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

В процессе осуществления образовательного процесса по дисциплине «Защита в операционных системах» используются:

-программное обеспечение для создания и демонстрации презентаций, иллюстраций и других учебных материалов:

- Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery);
- Microsoft OfficeSTD 2013;
- Dr. Web Desktop Security Suite;
- Kaspersky Endpoint Security;
- ViPNet Administrator 4.x (КС3;
- Сеть 11565. ViPNet Client for Windows 4.x (КС3);

- XSpyder 7.8.;
- СЗИ НСД Dallas Lock 8.0-K;
- Средства защиты информации Secret Net 7;
  -свободно распространяемый пакетный фильтр iptables;
  -свободно распространяемый прокси-сервер SQUID;
- Linux (GNU GPL v.3).

7. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная литература

1.Техническое противодействие компьютерной разведке: учебно-методическое пособие / Яросл. гос. ун-т им. П. Г. Демидова. Ч. 1 [Электронный ресурс]. / сост. Ю. И. Ушаков - Б.м.: Б.и., 2017. - 168 с.
http://www.lib.uniyar.ac.ru/edocs/iuni/20170209.pdf
2. Техническое противодействие компьютерной разведке: учебно-методическое пособие / Яросл. гос. ун-т им. П. Г. Демидова. Ч. 2 [Электронный ресурс]. / сост. Ю. И. Ушаков - Б.м.: Б.и., 2018. - 89 с.
http://www.lib.uniyar.ac.ru/edocs/iuni/20180201.pdf
3. Платонов В.В., «Программно-аппаратные средства защиты информации», учебник для студ. учреждений высш. проф. образования, М.: Издательский центр «Академия», 2014.- 336с.
4. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ.
5. Проскурин В.Г., «Защита программ и данных», 2-е издание, учебное пособие для студ. учреждений высш. проф. образования, М., Издательский центр «Академия», 2012.- 208с
6. Шелухин О.И. Системы обнаружения вторжений в компьютерные сети [Электронный ресурс] : учебное пособие / О.И. Шелухин, А.Н. Руднев, А.В. Савелов. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2013. — 88 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63360.html
7. Указ президента России от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности российской Федерации».

б) дополнительная литература

1. Касперски Крис Фундаментальные основы хакерства. Искусство дизассемблирования [Электронный ресурс] / Крис Касперски. — Электрон. текстовые данные. — М. : СОЛОН-ПРЕСС, 2010. — 446 c. — 5-93455-175-2. — Режим доступа: http://www.iprbookshop.ru/65405.html

в) ресурсы сети «Интернет»

1. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php).
2.Информационная система "Единое окно доступа к образовательным ресурсам" (http://www.edu.ru (раздел Учебно-методическая библиотека) или по прямой ссылке http://window.edu.ru/library).
3. Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru).
4. Новости в сфере угроз безопасности и защиты компьютерной информации российских журнала «Хакер»:https://xakep.ru/tag/news и журнала «Информационная безопасность»: http://itsec.ru/main.php.
5. Новейшие данные об угрозах работы с подключением к сети Интернет российской компании «Лаборатория Касперского»:http://www.kaspersky.ru/internet-security-center.

6. Материалы ежегодного всемирного конгрессахакеров «ChaosCommunicationCongress» в Гамбурге (на английском языке), где рассказывается о новых методах компьютерной выявленных разведки и выявленных уязвимостях в аппаратных решениях и программномобеспечении: https://events.ccc.de/congress/2015/wiki/Static:Main_Page, видеоматериалы с субтитрами конгресса ССС: https://www.youtube.com/user/CCCen/videos.
7. Федеральный банк данных угроз безопасности, ведущийся в разделе «Техническая защита информации» официального сайта ФСТЭК России (https://bdu.fstec.ru).
8. Сайт Федеральной службы технического и экспортного контроля Российской Федерации (https://fstec.ru) для знакомства с нормативными документами ФСТЭК России

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:
-учебные аудитории для проведения занятий лекционного типа, оборудованная персональной компьютерной техникой с установленными средствами визуализации текстов в формате DOC/DOCX, PDF, F2B, файлов изображений, презентаций, видео и других мультимедийных файлов, а также - видеопроектором и жалюзи на окнах, или компьютерной техникой и интерактивной компьютерной доской;

-учебные аудитории для проведения практических занятий: кабинет сетевых компьютерных технологий, лаборатории безопасности компьютерных сетей и программно-аппаратных средств обеспечения информационной безопасности(операционные системы Microsoft Windows и Linux, российские системы обнаружения вторжений и противодействия программным закладкам, антивирус лаборатории Касперского и средства криптозащиты «доктор ВЭБ");
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
-помещения для самостоятельной работы;
-помещения для хранения и профилактического обслуживания технических средств обучения.

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

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор(ы) :

Старший преподаватель кафедры Компьютерная безопасность и математические методы обработки информации Ю.И. Ушаков

)

Приложение №1 к рабочей программе дисциплины
«Техническое противодействие компьютерной разведке»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1 Контрольные задания и иные материалы, используемые в процессе текущей аттестации

Задания для самостоятельной работы

Варианты заданий выдаются учащимся на последнем часе лекционных занятий по теме. Оценка и обсуждение выполненных студентами заданий по самостоятельной работе производится на практическом занятии по данной теме и учитывается на ряду с результатами практических занятий при выставлении оценки текущей успеваемости.

Задания по теме № 1 «Цели и задачи компьютерной разведки, формы и условия ее проведения. Роль, место и формы противодействия компьютерной разведке»:

Вариант №1. Самостоятельно найти в открытых источниках примеры использования средств конкурентной компьютерной разведки, обосновать свой выбор.

Вариант №2. Самостоятельно найти в открытых источниках примеры использования методов компьютерной разведки для достижения политических целей, обосновать свой выбор.

Вариант №3. Самостоятельно найти в открытых источниках примеры использования методов компьютерной разведки для реализации идеологии терроризма, или экстремизма, обосновать свой выбор.

Вариант №4. Самостоятельно найти в открытых источниках пример противодействия государства использованию методов компьютерной разведки на организационно-правовом уровне, оценить эффективность принятых мер безопасности.

Вариант №5. Самостоятельно найти в открытых источниках пример технического противодействия государства использованию методов компьютерной разведки во враждебных России целях, оценить эффективность принятых мер безопасности.

Задания по теме № 2 «Методы выявления признаков и фактов проведения компьютерной разведки»:

Вариант № 1. Привести примеры программ-анализаторов сетевого трафика, которые можно использовать в интересах выявления признаков и фактов проведения компьютерной разведки.

Вариант № 2. На основании самостоятельной углубленной проработки Руководящего документа гостехкомиссии России (ФСТЭК России) от 04.06.1999г. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», привести признаки, которые могут свидетельствовать о проведении компьютерной разведки. Обосновать ответ.

Вариант № 3. На основе углубленной проработки учебно-методических материалов подготовить краткое описание стадий и признаков предварительной подготовки к проведению компьютерной разведки? Обоснуйте ответ.

Вариант № 4. На основе углубленной проработки учебно-методических материалов и положений Руководящего документа гостехкомиссии России (ФСТЭК России) от 04.06.1999г. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», привести и обосновать критерии аномального поведения сетевого трафика, подозрительного на проведение компьютерной разведки, методы его выявления.

Вариант № 5. На основе углубленной проработки учебно-методических материалов и Руководящего документа гостехкомиссии России (ФСТЭК России) от 04.06.1999г. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», привести и обосновать методы выявления аномальной работы процессора ПЭВМ, выделенной для практики, которая не может быть оправдана имеющимися активными и фоновыми задачами.

Задания по теме № 3 «Оценка уязвимости систем для компьютерной разведки»:

Вариант № 1. На основе углубленной проработки учебно-методических материалов и положений ГОСТ Р ИСО/МЭК 18045-2013г., «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий», выяснить какие шаги применяются для оценки рисков? Обосновать перечень.

Вариант № 2. На основе углубленной проработки учебно-методических материалов и положений ГОСТ Р ИСО/МЭК 18045-2013г., «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий», выяснить как производится идентификация уязвимостей системы от средств компьютерной разведки?

Вариант № 3. На основе углубленной проработки учебно-методических материалов пособия для вузов «Управление рисками информационной безопасности» (Милославская Н.Г., Сенаторов М.Ю., Толстой А.И., Учебное пособие для вузов, 2-е издание - испр., Серия «Вопросы управления информационной безопасностью. Выпуск 2, М.: «Горячая линия – Телеком», 2014. - 130с.), выяснить «шаги» методологии уменьшения риска, вычленив из нее риски связанные с применением средств и методов компьютерной разведки.

Вариант № 4. На основе углубленной проработки учебно-методических материалов пособия для вузов «Управление рисками информационной безопасности» (Милославская Н.Г., Сенаторов М.Ю., Толстой А.И., Учебное пособие для вузов, 2-е издание - испр., Серия «Вопросы управления информационной безопасностью. Выпуск 2, М.: «Горячая линия – Телеком», 2014. - 130с.), выяснить - что (какие данные) должно включать в себя утверждение в результатах оценки рисков применения методов компьютерной разведки (утверждение формулируется в виде пары: угроза применения компьютерной разведки-уязвимость)?

Вариант № 5. Совместно с представителями УЦИ ЯрГУ на математическом факультете и факультете ИВТ провести осмотр и проверку технического состояния средств защиты фрагмента сети учебного корпуса № 7 от средств и методов компьютерной разведки. На основе полученных данных, с учетом ГОСТ Р ИСО/МЭК 18045-2013г., «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий», составить для УЦИ ВУЗа анализ защищенности данного сетевого фрагмента.

Задания по теме № 4 «Средства и методы обнаружения вторжений в информационные системы»:

Вариант № 1. На основе углубленной проработки учебно-методических материалов и положений ГОСТ Р ИСО/МЭК 53113-2-2009 «Информационные технологии. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов. Часть 2. Рекомендации по защите информации, информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов», выяснить и кратко охарактеризовать технологии построения систем обнаружения атак (как метода компьютерной разведки).

Вариант № 2. На основе углубленной проработки учебно-методических материалов из перечня основной и дополнительной литературы, укажите сильные и слабые стороны методов обнаружения аномалий, применяемых для выявления компьютерной разведки. Обосновать ответ.

Вариант № 3. На основе углубленной проработки учебно-методических материалов перечислите и кратко охарактеризуйте методы интеллектуального анализа данных в системах обнаружения вторжений. Приведите примеры перспективных научно-технических разработок применения интеллектуальных систем для обнаружения признаков вторжений. Обосновать ответ.

Вариант № 4. На основе углубленной проработки рекомендованных учебно-методических материалов из перечней основной и дополнительной литературы приведите примеры и проиллюстрируйте роль мониторинговых программ в выявлении аномалий в работе информационных систем. Обосновать ответ.

Вариант № 5. На основе углубленной проработки рекомендованных учебно-методических материалов по профилям защиты информационных систем 4-го, 5-го и 6-го классов из нормативных документов ФСТЭК России «Требования к системам обнаружения вторжений», введенных приказом ФСТЭК России от 6 декабря 2011 г. № 638 (зарегистрирован Минюстом России 1 февраля 2012 г., per. №23088), приведите обоснование различий в требованиях к указанным классам ИС.

Задания по теме № 5«Противодействие программным закладкам»**:**

Вариант № 1. На основе углубленной проработки рекомендованных учебно-методических материалов из перечней основной и дополнительной литературы, дайте развернутое определение - как формально определяется модель компьютерной разведки «наблюдатель» и какие у нее имеются типичные недостатки?

Вариант № 2. На основе углубленной проработки рекомендованных учебно-методических материалов из перечней основной и дополнительной литературы, дайте развернутое определение - как формально определяются модели компьютерной разведки «перехват», «уборка мусора» и «мониторы файловых систем». В чем их суть и признаки использования?

Вариант № 3. На основе углубленной проработки рекомендованных учебно-методических материалов из перечней основной и дополнительной литературы, дайте развернутое определение и обоснуйте - в чем сильные и слабые стороны сигнатурного и эвристического сканирования как метода противодействия программным закладкам?

Вариант № 4. На основе углубленной проработки рекомендованных учебно-методических материалов из перечней основной и дополнительной литературы, дайте развернутое определение - какие сильные и слабые стороны имеет метод выявления программных закладок «сканирование на лету»?

Вариант № 5. На основе углубленной проработки рекомендованных учебно-методических материалов из перечней основной и дополнительной литературы, дайте развернутое определение и обоснование - какие сильные и слабые стороны имеет метод выявления программных закладок «контроль целостности конфигурации системы»?

Задания по теме № 6 «Комплекс мер противодействия компьютерной разведке»

Вариант №1. Проведите по открытым источника, включая материалы сети Интернет по конкурентной разведке самостоятельный поиск авторских семинаров о приемах такой разведки и составьте их примерный перечень, выделив и обосновав отдельные этапы.

Вариант № 2. На основе углубленной проработки рекомендованных учебно-методических материалов, Федерального закона от 27.07.2017 № 187-фз и перечня требований ФСТЭК России по защищенности критической информационной инфраструктуры, дайте развернутое определение перечня работ, средств и методов защиты указанных КС КИИ от компьютерных атак.

Вариант №3. На основе углубленной проработки учебно-методических материалов, федеральных законов и нормативных требований ФСТЭК России по защищенности критической информационной инфраструктуры, дайте развернутое определение организационному комплексу мер, принимаемый в России для противодействия компьютерной разведке.

Вариант №4. На основе углубленной проработки учебно-методических материалов, проведите самостоятельный поиск в сети Интернет актуальных российских программно-аппаратных решений противодействия методам компьютерной разведки. Составьте по ним небольшой доклад и презентацию.

Вариант № 5. На основе углубленной проработки рекомендованных учебно-методических материалов, Федерального закона от 27.07.2017 № 187-фз и перечня требований ФСТЭК России по защищенности критической информационной инфраструктуры, используя отрытые сведения и официальные документы в сети Интернет, охарактеризуйте систему защиты регионального фрагмента информационной инфраструктуры крупнейшего федерального оператора связи ПАО «Ростелеком».

Задания по теме № 7 «Методы управления информационной безопасностью»

Вариант № 1. На основе углубленной проработки учебно-методических материалов и «Доктрины информационной безопасности российской Федерации» (Указ Президента России № 646 от 05.12.2016) составить современный вариант организационной составляющей структуры обеспечения информационной безопасности России с учетом новейших угроз безопасности от санкционной политики и информационной войны.

Вариант № 2. На основе углубленной проработки учебного пособия для вузов Курило А.П, Милославской Н.Г., Сенаторова М.Ю., Толстого А.И., «Основы управления информационной безопасностью» Серия «Вопросы управления информационной безопасностью. Выпуск 1.», «Доктрины информационной безопасности российской Федерации» (Указ Президента России № 646 от 05.12.2016) и с учетом новейших угроз безопасности от санкционной политики и информационной войны, составить современный вариант локальной организационно-технической составляющей структуры обеспечения информационной безопасности отдельных фрагментов государственных ИС в субъекте Федерации.

Вариант № 3. На основе углубленной проработки рекомендованных учебно-методических материалов, Федерального закона от 27.07.2017 № 187-фз и перечня требований ФСТЭК России по защищенности критической информационной инфраструктуры, с учетом новейших угроз безопасности от санкционной политики и информационной войны, составить современный вариант локальной организационно-технической составляющей структуры обеспечения информационной безопасности отдельного объекта критической информационной инфраструктуры.

Вариант № 4. На основе углубленной проработки рекомендованных учебно-методических материалов из перечней основной и дополнительной литературы составить краткий доклад о схожести и различиях в российских и международных стандартах управления информационной безопасностью.

Вариант № 5. На основе углубленной проработки Учебного пособия для вузов Милославской Н.Г., Сенаторова М.Ю. и Толстого А.И., «Проверка и оценка деятельности по управлению информационной безопасности» серия «Вопросы управления информационной безопасностью. Выпуск 5.», с учетом новейших угроз безопасности от санкционной политики и информационной войны, составить примерный план поддержания адекватной политики информационной и компьютерной безопасности на защищаемых российских объектах информатизации, предусмотрев контроль за ее эффективностью и меры совершенствования.

1.2 Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к зачету

1. Задачи проведения компьютерной разведки. Факторы и условия, облегчающие ее проведение.
2. Меры организационно-правового характера, используемые в России для противодействия компьютерной разведке.
3. Меры инженерно-технического характера, применяемые в мире для противодействия компьютерной разведке. Российские особенности форм и методов, используемых для технического противодействия компьютерной разведке.
4. Обобщенный сценарий атаки при проведении компьютерной разведке. Охарактеризовать все шесть его шагов. В чем заключаются признаки каждого из шагов?
5. Классификация типичных удаленных атак. Охарактеризуйте таксономию атак по схеме: -угрозы, средства, получение доступа к…, результаты, цели.
6. Применение онтологии для классификации атак компьютерной разведки по их цели.
7. Оценивание степени серьезности атак компьютерной разведки.
8. Использование программ анализа и мониторинга сетевого трафика для выявления признаков и фактов проведения компьютерной разведки.
9. Какие данные используются и как они готовятся для выявления и изучения аномалий сетевого трафика, подозрительных на применение компьютерной разведки.
10. Использование статистического метода для выявления аномального поведения программ, подозрительного на применение компьютерной разведки.
11. Обнаружения аномалий (подозрительных на применение компьютерной разведки) методом главных компонент.
12. Алгоритм обнаружения аномалий (подозрительных на применение компьютерной разведки) методом дискретного вейвлет-преобразования.
13. Идентификация уязвимостей системы от средств компьютерной разведки.
14. Содержание утверждений в результатах оценки рисков применения методов компьютерной разведки (утверждение формулируется в виде пары: угроза применения компьютерной разведки-уязвимость). Обосновать выбор из общего перечня рисков.
15. Методология уменьшения рисков, связанных с применением средств и методов компьютерной разведки.
16. Технологии построения систем обнаружения атак, характерных для проведения компьютерной разведки.
17. Сильные и слабые стороны методов обнаружения аномалий, применяемых для выявления компьютерной разведки.
18. Охарактеризовать методы интеллектуального анализа данных в системах обнаружения вторжений.
19. Метод Data Maining, применяемый в системах обнаружения вторжений, характерных для компьютерной разведки.
20. Метод опорных векторов, применяемый в системах обнаружения вторжений, характерных для компьютерной разведки.

21. Применение нейронных сетей для обнаружения аномалий трафика, характерного для компьютерной разведки.
22. Методы искусственного интеллекта в задачах обеспечения безопасности сетей от компьютерной разведки.
23. Методы искусственных иммунных систем и нейронных сетей для обнаружения атак, характерных для компьютерной разведки.
24. Преобразования Хафа и его использования для обнаружения аномалий трафика, характерных для компьютерной разведки.
25. Модели компьютерной разведки «перехват», «уборка мусора» и «мониторы файловых систем». В чем их суть и признаки использования?
26. Методы «обхода» сетевых и хостовых систем обнаружения вторжений, используемые компьютерной разведкой.
27. Методы защиты от программных закладок. Их назначения и суть для противодействия компьютерной разведке.
28. Сигнатурное и эвристическое сканирование как методы противодействия программным закладкам.
29. Метод выявления программных закладок «сканирование на лету». В чем суть и признаки использования метода для выявления компьютерной разведки?
30. Метод выявления программных закладок «контроль целостности конфигурации системы». В чем суть и признаки использования метода для выявления компьютерной разведки?
31. Защита от программных закладок ранее неизвестных типов. Обнаружение программных закладок, скрытых с помощью стелс-технологий.
32. Использование программ-ловушек для противодействия программным закладкам.
33. Понятия и причины разработки политики информационной безопасности. Политика информационной безопасности организации. Причины выработки политики информационной безопасности.
34. Требования и принципы, учитываемые при разработке политики информационной безопасности.
35. Содержание политики информационной безопасности организации.
36. Система управления информационной безопасностью организации.
36. Процессный подход к управлению информационной безопасностью организации.
37. Работа с процессами системы управления информационной безопасностью организации.
38. Стратегии построения и внедрения системы управления информационной безопасностью организации.
39. Системный подход к управлению рисками информационной безопасности.
40. Установление контекста управления рисками информационной безопасности.
41. Содержание двух этапов оценки рисков информационной безопасности.
42. Содержание оценки и анализа рисков информационной безопасности. Обработка рисков.
43. Понятие рисков информационной безопасности, коммутация рисков, мониторинг рисков ИБ и их пересмотр.
44. Обеспечение управления рисками информационной безопасности организации.
45. Управление инцидентами информационной безопасности организации.
46. Управление непрерывностью бизнеса организации.
47. Роль «Доктрины информационной безопасности российской Федерации» (объявленной указом президента России от 05.12.2016 № 646) в системе обеспечения безопасности объектов информационной инфраструктуры России.
48. Роль Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ в системе

обеспечения безопасности объектов критической информационной инфраструктуры России.
49. Роль ГОСТ Р ИСО/МЭК ТО 19791-2008г. «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» и ГОСТ Р ИСО/МЭК 18045-2013г., «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» при оценке защищенности объектов информационной инфраструктуры России.
50. Роль руководящего документа ФСТЭК России «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» в системе противодействия методам компьютерной разведки.
51. Роль руководящего документа ФСТЭК России об утверждении «Требований к средствам антивирусной защиты» в системе противодействия методам компьютерной разведки.
52. Роль руководящего документа ФСТЭК России об утверждении «Требований к системам обнаружения вторжений» в системе противодействия методам компьютерной разведки.

2. Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

2.1 Шкала оценивания сформированности компетенций и ее описание

Оценивание уровня сформированности компетенций в процессе освоения дисциплины осуществляется по следующей трехуровневой шкале:

Пороговый уровень - предполагает отражение тех ожидаемых результатов, которые определяют минимальный набор знаний и (или) умений и (или) навыков, полученных студентом в результате освоения дисциплины. Пороговый уровень является обязательным уровнем для студента к моменту завершения им освоения данной дисциплины.

Продвинутый уровень - предполагает способность студента использовать знания, умения, навыки и (или) опыт деятельности, полученные при освоении дисциплины, для решения профессиональных задач. Продвинутыйуровеньпревосходит пороговый уровень по нескольким существенным признакам.

Высокий уровень - предполагает способность студента использовать потенциал интегрированных знаний, умений, навыков и (или) опыта деятельности, полученных при освоении дисциплины, для творческого решения профессиональных задач и самостоятельного поиска новых подходов в их решении путем комбинирования и использования известных способов решения применительно к конкретным условиям. Высокий уровень превосходит пороговый уровень по всем существенным признакам.

2.2 Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования

Код компе-тенции	Форма контроля	Этапы форми-рования (№ темы (раздела)	Показатели оценивания	Шкала и критерии оценивания компетенций на различных этапах их формирования		
				Пороговый уровень	Продвинутый уровень	Высокий уровень
Профессиональные компетенции						
ПК-12	Опрос по заданиям для самостоятельной работы по темам № 1-5, зачет	1-7	**Знать** методы проведения инструментального мониторинга защищенности компьютерных систем.	**Знание** основных методов проведения инструментального мониторинга защищенности компьютерных систем.	**Знание** основных и специальных методов проведения инструментального мониторинга уязвимости и защищенности компьютерных систем.	**Знание** основных и специальных методов проведения инструментального мониторинга уязвимости, защищенности компьютерных систем, а также вероятностей реализации угроз, анализа рисков и сведения их к минимуму.
	Опрос по заданиям для самостоятельной работы по темам № 1-5, зачет	1-7,	**Уметь** применять специальные методы и средства для инструментального мониторинга защищенности компьютерных систем.	**Умение** применять основные методы инструментального мониторинга защищенности компьютерных систем.	**Умение** применять основные и специальные методы и средства для инструментального мониторинга уязвимости и защищенности компьютерных систем.	**Умение** применять основные и специальные методы и средства для инструментального мониторинга уязвимости и защищенности компьютерных систем, а также обоснованно рассчитывать вероятности реализации угроз, проводить анализ рисков и использовать средства сведения их к приемлемому уровню.
	Опрос по заданиям для самостоятельной работы по темам № 1-5, зачет	1-7	**Владеть навыками** проведения инструментального мониторинга защищенности компьютерных	**Владение навыками** использования основных методов инструментального мониторинга защищенности	**Владение навыками** использования основных и специальных методов и средств инструментального мониторинга уязвимости	**Владение навыками** использования специальных методов и средств инструментального мониторинга уязвимости и защищенности компьютерных

			систем.	компьютерных систем.	и защищенности компьютерных систем.	систем, а также обоснованно рассчитывать вероятности реализации угроз, проводить анализ рисков и использования стандартных средств сведения их к приемлемому уровню.
ПК-19	Опрос по заданиям для самостоятельной работы по темам № 1-5, зачет	1 – 7	**Знать:** – формы проведения проверки технического состояния средств защиты информации; -методы и способы проведения профилактических осмотров технических средств защиты информации.	**Знание:** – основных форм проведения проверки технического состояния средств защиты информации; - основных методов и способов проведения профилактических осмотров технических средств защиты информации.	**Знание** основных методов, способов и форм проведения проверок технического состояния и профилактических осмотров аппаратно-программных средств защиты информации.	**Знание** основных и специальных методов, способов и форм проведения проверок технического состояния и профилактических осмотров аппаратно-программных средств защиты информации, соответствия их настроек уровню угроз безопасности.
	Опрос по заданиям для самостоятельной работы по темам № 1-5, зачет	1-7	**Уметь** проводить проверки технического состояния и профилактические осмотры технических средств защиты информации.	**Умение** проводить типичные проверки технического состояния и профилактические осмотры технических средств защиты информации.	**Умение** проводить типичные и специальные проверки технического состояния и профилактические осмотры аппаратно-программных средств защиты информации.	**Умение** проводить типичные и специальные проверки технического состояния и профилактические осмотры аппаратно-программных средств защиты информации, соответствия их настроек уровню угроз безопасности.
	Опрос по заданиям для самостоятельной работы по темам № 1-5, зачет	1-7	**Владеть навыками** проведения проверок технического состояния и профилактических осмотров технических средств защиты информации.	**Владение навыками** проводить типичные проверки технического состояния и профилактические осмотры технических средств защиты информации.	**Владение навыками** проводить типичные и специальные проверки технического состояния и профилактические осмотры аппаратно-программных средств защиты информации.	**Владение навыками** проводить типичные и специальные проверки технического состояния и профилактические осмотры аппаратно-программных средств защиты информации, соответствия их настроек уровню угроз безопасности.

3. Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

3.1 Критерии оценивания степени овладения знаниями, умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

- владение основным объемом знаний по программе дисциплины;
- знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;
- владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;
- способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой дисциплины;
- знание базовых теорий, концепций и направлений по изучаемой дисциплине;
- достаточный уровень культуры исполнения заданий для самостоятельной работы, периодическое участие в групповых обсуждениях хода и результатов их выполнения.

Продвинутый уровень (общие характеристики):

- достаточно полные и систематизированные знания в объёме программы дисциплины;
- использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- владение инструментарием дисциплины, умение его использовать в решении учебных задач;
- способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;
- высокий уровень культуры исполнения заданий для самостоятельной работы, периодическое участие в групповых обсуждениях хода и результатов их выполнения.

Высокий уровень (общие характеристики):

- систематизированные, глубокие и полные знания по всем разделам дисциплины;

- точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;
- безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;
- способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;
- высокий уровень культуры исполнения заданий для самостоятельной работы, активное творческое участие в групповых обсуждениях хода и результатов их выполнения.

3.2 Описание процедуры выставления оценки

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка. Для дисциплин, изучаемых в течение нескольких семестров, оценка может выставляться не только по окончании ее освоения, но и в промежуточных семестрах. Вид оценки («отлично», «хорошо», «удовлетворительно», «неудовлетворительно», «зачтено», «не зачтено») определяется рабочей программой дисциплины в соответствии с учебным планом, - в зависимости от того, в каком статусе преподается дисциплина, – по выбору из набора дисциплин вариативной части, либо в качестве дисциплины основной части (в этом случае проводится дифференцированный зачет).

Оценка «отлично» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована на высоком уровне.

Оценка «хорошо» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на продвинутом уровне.

Оценка «удовлетворительно» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «неудовлетворительно» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Оценка «зачет» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «не зачтено» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Приложение № 2 к рабочей программе дисциплины
«Техническое противодействие компьютерной разведке»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Техническое противодействие компьютерной разведке» являются лекции, причем в достаточно большом объеме. Это связано с тем, что в основе данная дисциплина находится как бы на стыке между дисциплинами «Техническая защита информации» в части защиты от технической разведки в специфической области компьютерной безопасности, и циклом дисциплин «Защита программ и данных», «Защита в операционных системах», «Основы построения защищенных компьютерных сетей» и «Основы построения защищенных баз данных». Также она использует частично материал дисциплины «Организационно-правовое обеспечение информационной безопасности». Для успешного освоения дисциплины важноуглубленное изучение некоторых разделов указанных дисциплин, как в аудитории, так и самостоятельно, в качестве выполняемых в домашних условияхзаданий.

Основная цель самостоятельных работ – помочь усвоить теоретические основы и практическиеметоды противодействия компьютерной разведке. Для этого необходимо знать и понимать лекционный материал. Поэтому, в процессе изучения дисциплины, рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, представленный в предлагаемой учебной литературе, необходимо дома еще раз прорабатывать и, при необходимости, дополнять информацией, полученной на консультациях, практических занятиях и из рекомендованных ресурсов сети «Интернет».

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков использованияучебной литературы, в течение обучения проводятся мероприятия текущей аттестации в виде самостоятельных работ (в домашних условиях). Варианты заданий выдаются учащимся на последнем часе лекционных занятий по каждой значимой теме. Оценка и обсуждение выполненных студентами заданий по самостоятельной работе производится на практических занятиях и учитывается, на ряду с результатами практических занятий, при оценке текущей успеваемости. Также проводятся консультации (при необходимости) по разбору заданий для самостоятельной работы, которые вызвали затруднения.

В конце семестра изучения дисциплины студенты сдают зачет. Зачет принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса. На самостоятельную подготовку к зачету выделяется 3дня, во время подготовки к зачету предусмотрена групповая консультация.

Самостоятельно освоить вопросы дисциплины «Техническое противодействие компьютерной разведке» студенту крайне сложно. Это обусловлено тем, что студенты слабо представляют объемы и характер реально проводимой компьютерной конкурентной разведки, хакерства из меркантильных побуждений, использования методов компьютерной разведки террористами и экстремистами из-за ее скрытности, а такжеисключительную изощренность научной и политической компьютерной разведки, проводимой спецслужбами иностранных государств на основе «багов» и «эксплойтов», заложенных зарубежными производителями аппаратно-программных решений в соответствии с законодательством по национальной безопасности. Поэтому,является совершенно необходимым посещение студентамивсех аудиторных занятий, где им прививается патриотизм и непримиримость к любым аспектам иностранного проникновения для доступа к защищаемой информации и управления российскими информационными системами, идеология противодействия методам компьютерной разведки и, на этой основе, разъясняются учебные вопросы.

Учебно-методическое обеспечение
самостоятельной работы студентов по дисциплине

Для самостоятельной работы особенно рекомендуется использовать литературу и интернет-источники, указанные в разделе 7.