Минобрнауки России
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

УТВЕРЖДАЮ
Проректор по учебной работе

_____ _Василенко В.Н._
(подпись) (Ф.И.О.)

«26» мая 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Система обнаружения компьютерных атак

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация (степень) выпускника

специалист по защите информации

Разработчик _____ _____ ____Белокуров С.В..____
(подпись) (дата) (Ф.И.О.)

СОГЛАСОВАНО:

Заведующий кафедрой __Информационной безопасности_____
(наименование кафедры, являющейся ответственной за данное направление подготовки, профиль)

_____ _____ _____Скрыпников А. В._____
(подпись) (дата) (Ф.И.О.)

1. Цели и задачи дисциплины

Целями и задачи дисциплины «Система обнаружения компьютерных атак» в соответствии с видами профессиональной деятельности являются:

- эксплуатационную:

- реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;

- в соответствии со специализацией №4 «Безопасность открытых систем»:

- проектирование, эксплуатация и совершенствование системы управления информационной безопасностью открытой информационной системы.

Объектами профессиональной деятельности являются:

– автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности автоматизированных систем;

– системы управления информационной безопасностью автоматизированных систем.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

№ п/п	Компетенция	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ПК-3	способностью проводить анализ защищенности автоматизированных систем	основные задачи администрирования подсистемы ИБ объекта защита; инструменты администрирования;	проводить анализ угроз безопасности автоматизированных систем	моделями, методами и инструментами многослойной защиты информации
2	ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Описание уязвимостей рассматриваемого объекта или ресурса.	использовать методы оценки уязвимости защищаемых персональных данных, построения модели угроз	методами построения модели угроз и нарушителей.
3	ПК-13	способностью участвовать в проектировании средств защиты информации автоматизированной системы	системы, комплексы и средства обеспечения информационной безопасности	проектировать комплексную систему защиты информации и информационных систем	методами и средствами проектирования систем обеспечения информационной безопасности и защиты информационных систем
4	ПК-14	способностью проводить контрольные проверки работоспособ-	основные программные, программно- аппаратные и технические	организовывать и проводить контрольные проверки работоспособности	методами и инструментами оценки эффективности

		ности применяемых программно-аппаратных, криптографических и технических средств защиты информации	средства защиты информации; основные метрологические показатели средств защиты информации	средств защиты информации	
5	ПК-15	способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	основные нормативные акты сертификации	находить и определять область применения различных категорий и видов стандартов, систем стандартов, классификаторов и указателей, документацией продукции, процессов, услуг и систем качества	навыками использования различных категорий и видов стандартов, систем стандартов, классификаторов и указателей, документацией продукции, процессов, услуг и систем качества
6	ПК-22	способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	основные средства и способы обеспечения ИБ, принципы построения системы защиты ИБ	разрабатывать частные политики информационной безопасности информационных систем;	навыками разработки документирования, тестирования и отладки программного обеспечения по защите информации
7	ПК-23	способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	применять методы и способы защиты информации в информационных системах персональных данных	определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем;	навыками анализа информационной инфраструктуры информационной системы и ее безопасности
8	ПК-24	способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	принципы организации информационны х систем в соответствии с требованиями по защите информации	разрабатывать частные политики информационной безопасности информационных (автоматизированных) систем	профессиональной терминологией в области информационной безопасности
9	ПК-25	способностью обеспечить эффективное применение средств	принципы организации информационных систем в соответствии с	разрабатывать предложения по совершенствованию системы управления	навыками выбора и обоснования критериев эффективности функционирования

		защиты информационно- технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных	требованиями по защите информации	информационной безопасностью автоматизированных систем	защищенных информационных (автоматизированных) систем
10	ПК-27	способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	подходы к формированию и реализации политики информационной безопасности автоматизированных систем	составлять политики информационной безопасности для автоматизированных систем и применять их на практике	навыками составления и использования политик информационной безопасности
11	ПК-28	способностью управлять информационной безопасностью автоматизированной системы	комплекс мероприятий по обеспечению информационной безопасности автоматизированных систем	определять перспективные направления и пути совершенствования автоматизированной системы	навыками участия в формировании, организации и поддержки комплекса мер по обеспечению информационной безопасности автоматизированной системы

3. Место дисциплины в структуре ОП ВО

Дисциплина «Система обнаружения компьютерных атак» относится к блоку 1 ОП и ее базовой части.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися базового школьного курса или освоении программы СПО.

Дисциплина является предшествующей для изучения дисциплин, прохождения практик:

- Безопасность сетей ЭВМ;
- Безопасность систем баз данных;
- Виртуальные частные сети;
- Защита web-сайтов;
- Защита конфиденциальной информации;
- Информационная безопасность открытых систем;
- Криптографические протоколы и стандарты;
- Криптографические методы защиты информации;
- Основы спектрального анализа;
- Программно-аппаратные средства обеспечения информационной безопасности;
- Разработка и эксплуатация защищенных автоматизированных систем;

– Сети и системы передачи информации;
– Техническая защита информации;
– Элементы теории графов и сетей в математических пакетах;
– Учебная практика, практика по получению первичных профессиональных умений;
– Учебная практика, практика по получению первичных умений и навыков научно-исследовательской деятельности;
– Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности;
– Производственная практика, преддипломная практика;
защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 4 зачетные единицы.

Виды учебной работы	**Всего часов**	**Семестр**
		4
	акад. ч	акад. ч
Общая трудоемкость дисциплины	144	144
Контактная работа, в т.ч. аудиторные занятия	**55**	**55**
Лекции	18	18
в том числе в форме практической подготовки	–	–
Практические занятия (ПЗ)	36	36
в том числе в форме практической подготовки	36	36
Консультации текущие	0,9	0,9
Вид аттестации – зачет	0,1	0,1
Самостоятельная работа:	**89**	**89**
Проработка лекций, учебников (собеседование, коллоквиум)	40	40
Домашнее задание	49	49

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

5.1 Содержание разделов дисциплины

№ п/п	Наименование разделов дисциплины	Содержание раздела	Трудоемкость раздела, час
1	Теоретические основы	Модель OSI. Оборудование локальных сетей.	26
2	Классификация атак по уровням иерархической модели OSI	Атаки на физическом уровне. Атаки на канальном уровне; Атаки на сетевом уровне; Атаки на транспортном уровне; Безопасность прикладного уровня.	84
3	Уязвимости	Основные типы уязвимостей.	34

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ПЗ, час	СР, час
1	Теоретические основы	2	4	20
2	Классификация атак по уровням иерархической модели OSI	10	24	50
3	Уязвимости	6	8	20

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость час
1	Теоретические основы	Модель OSI: Прикладной (7) уровень (Application Layer); представительский (6) уровень (Presentation Layer); Сеансовый (5) уровень (Session Layer); Транспортный (4) уровень (Transport Layer); Сетевой (3) уровень (Network Layer); Канальный (2) уровень (Data Link Layer); Физический (1) уровень (Physical Layer)	2
2	Классификация атак по уровням иерархической модели OSI	Атаки на физическом уровне. Концентраторы. Атаки на канальном уровне; Атаки на коммутаторы; Переполнение CAM-таблицы. VLAN Hoping Атака на STP; MAC Spoofing;Атака на PVLAN (Private VLAN) Атака на DHCP; ARP-spoofing; Атаки на сетевом уровне; Атаки на маршрутизаторы; Среды со статической маршрутизацией; Безопасность статической маршрутизации; Среды с динамической маршрутизацией; Scapy - универсальное средство дли реализации сетевых атак; Среды с протоколом RIP; Безопасность протокола RIP; Ложные маршруты RIP; Понижение версии протокола RIP; Взлом хэша MD5; Обеспечение безопасности протокола RIP; Среды с протоколом OSPF; Безопасность протокола OSPF; Среды с протоколом BGP; Атака BGP Router Masquerading; Атаки на MD5 для BGP; «Слепые» DoS-атаки на BGP- маршрутизаторы; Безопасность протокола BGP; Атаки на BGP; Атаки на транспортном уровне. Транспортный протокол TCP; Известные проблемы; Атаки на TCP; IP- spoofing; TCP hacking; Десинхронизация нулевыми данными; Сканирование сети; SYN-флуд; Атака Teardrop; Безопасность TCP; Атаки на уровне приложений. Безопасность прикладного уровня; Протокол SNMP; Протокол Syslog; Протокол DNS; Безопасность DNS; Веб- приложения; Атаки на веб через управление сессиями; Защита DNS; SQL-инъекции.	10
3	Уязвимости	Основные типы уязвимостей; Уязвимости проектирования; Уязвимости реализации; Уязвимости эксплуатации; Примеры уязвимостей; Права доступа к файлам; Оперативная память; Объявление памяти; Завершение нулевым байтом; Сегментация памяти программы; Переполнение буфера; Переполнения в стеке; Эксплоит без кода эксплоита; Переполнения в куче и bss; Перезапись указателей функций; Форматные строки; Сканирование приложений на наличие уязвимостей; Эксплуатация найденных уязвимостей; Защита от уязвимостей.	6

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Теоретические основы	Работа с операционными системами Linux Server и Windows Server. Основные команды, приемы администрирования. Основы администрирования промышленных СУБД.	4
2	Классификация атак по уровням иерархической модели OSI	Работа с дистрибутивом диагностики и защиты сетей Kali Linux.	24
3	Уязвимости	Антивирусная диагностика и защита	8

5.2.3Лабораторный практикум Не предусмотрен

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Теоретические основы	Проработка лекций, учебников (собеседование, коллоквиум)	10
		Подготовка отчетов по практической работе	10
2	Классификация атак по уровням иерархической модели OSI	Проработка лекций, учебников (собеседование, коллоквиум)	25
		Подготовка отчетов по практической работе	25
3	Уязвимости	Проработка лекций, учебников (собеседование)	10
		Подготовка отчетов по практической работе	10

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. – 2-е изд., перераб. и доп. – Москва : ДМК Пресс, 2017. – 434 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=566834 (дата обращения: 16.02.2020). – ISBN 978-5-97060-435-9.

2. Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. – Орел : МАБИВ, 2014. – 257 с. : табл., схем. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=428605 (дата обращения: 16.02.2020). – Текст : электронный.

3. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно- строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 16.02.2020). – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.

4. Левкина, А.О. Компьютерные технологии в научно- исследовательской деятельности: учебное пособие для студентов и аспирантов социально- гуманитарного профиля / А.О. Левкина. – Москва ; Берлин : Директ-Медиа, 2018. – 119 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=496112 (дата обращения: 15.01.2020). – Библиогр. в кн. – ISBN 978-5-4475-2826-3. – DOI 10.23681/496112. – Текст : электронный.

6.2. Дополнительная литература

1. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=429070 (дата обращения: 16.02.2020). – Библиогр. в кн. – Текст : электронный.

2. Громов, Ю.Ю. Основы Web-инжиниринга: разработка клиентских приложений / Ю.Ю. Громов, О.Г. Иванова, С.В. Данилкин ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». – Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2012. – 240 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=277648 (дата обращения: 15.01.2020). – Текст : электронный.

3. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 16.02.2020). – Библиогр. в кн. – Текст : электронный.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

Защита web-сайтов [Электронный ресурс]: методические указания для самостоятельной работы для студентов, обучающихся по направлению 10.05.03– «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников**,** Е. В. Чернышова ; ВГУИТ, Кафедра информационной безопасности. - Воронеж : ВГУИТ, 2016. - 20 с. http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/14820

6.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» - федеральный портал	*https://www.edu.ru/*
Научная электронная библиотека	*https://elibrary.ru/defaultx.asp*
Национальная исследовательская компьютерная сеть России	*https://niks.su/*
Информационная система «Единое окно доступа к образовательным ресурсам»	*http://window.edu.ru/*
Электронная библиотека ВГУИТ	*http://biblos.vsuet.ru/megapro/web*
Сайт Министерства науки и высшего образования РФ	*https://minobrnauki.gov.ru/*
Портал открытого on-line образования	*https://npoed.ru/*
Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ»	*https://education.vsuet.ru/*

6.5 Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс] : методические указания для обучающихся на всех уровнях высше- го образования / М. М. Данылив, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. - Воронеж: ВГУИТ, 2016. – Режим доступа: http://biblos.vsuet.ru/MegaPro/Web/SearchResult/Marc Format/ 2488. - Загл. с экрана

6.6 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При изучении дисциплины используется программное обеспечение и информационные справочные системы: информационная среда для дистанционного обучения «Moodle», локальная сеть университета и глобальная сеть Internet, Microsoft Office Professional Plus 2010 Microsoft Office Professional Plus 2007 Microsoft Visual Studio; IIS 7+; .NET 4+

7 Материально-техническое обеспечение дисциплины (модуля)

Аудитории для проведения занятий лекционного типа, лабораторных и практических занятий	*Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ-12 (компьютер Core i5-4460), проектор Acer projector X1383WH, экран, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГА-ТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-Р3.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920*	*Microsoft Windows 7 (64 разрядная) Профессиональная Лицензия (DreamSpark); Microsoft Office (standart) 2007 Профессиональная Лицензия (DreamSpark);Microsoft Access 2007 Профессиональная Лицензия (DreamSpark); Microsoft Project 2007 Профессиональная Лицензия (DreamSpark); Microsoft Share Point 2007 Профессиональная Лицензия (DreamSpark); Microsoft Visio 2007 Профессиональная Лицензия (DreamSpark) Microsoft SQL server 2008 Профессиональная Лицензия (DreamSpark); 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор)Бесплатное ПО; Adobe Acrobat Reader (Бесплатное ПО); Adobe Flash Player (Бесплатное ПО); FAR file managerБесплатное ПО; Google ChromeБесплатное ПО; Java TM 7 (64-bit)Бесплатное ПО; K-Lite Codec PackБесплатное ПО; Mozilla FirefoxБесплатное ПО; Oracle VM VirtualBoxБесплатное ПО; Sublime TextБесплатное ПО; Symantec Endpoint Protection 12(Заменен на AVP Kaspersky)Бесплатное ПО; VMWare Player (Бесплатное ПО); Антивирус “Зоркий глаз” (Бесплатное ПО); Lazarus (аналог Delphi)Бесплатное ПО; SmathStudio (аналог Mathcad)Бесплатное ПО; NanoCAD (аналог Autocad)Бесплатное ПО; Gimp (графичский редактор аналог Photoshop) Бесплатное ПО; Avidemax (видео редактор)Бесплатное ПО; Virtual Dub (видео редактор)Бесплатное ПО; Free Pascal (Бесплатное ПО); Страж NT вер.3.0 Сертификат ФСТЭК No 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК No 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК No 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК No1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК No3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК No1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК No2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК No2945 16.08.2013*
Аудитории для проведения занятий лекционного типа, лабораторных и практических занятий	*Ауд. 332а: Комплекты мебели для учебного процесса. ПЭВМ – 12 (компьютер Core i5-4570),средство активной защиты информации изделие «Салют 2000С» с регулятором выходного уровня шума, стенды – 5 шт. Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 12: рабочая станция CPU Core 2Duo E6300 – 1.86 – 10 шт, Celeron D2.8 – 2шт.; стенды – 3 Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ-12 (компьютер Core i5-4460), проектор Acer projector X1383WH, экран, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля*	*Microsoft Windows 7 (64 разрядная) Профессинальная Лицензия (DreamSpark); Microsoft Windows 2003 Профессиональная Лицензия (DreamSpark); Microsoft Office (standart) 2007 Профессиональная Лицензия (DreamSpark);Microsoft Access 2007 Профессиональная Лицензия (DreamSpark); Microsoft Project 2007 Профессиональная Лицензия (DreamSpark); Microsoft Share Point 2007 Профессиональная Лицензия (DreamSpark); Microsoft Visio 2007 Профессиональная Лицензия (DreamSpark) Microsoft SQL server 2008 Профессиональная Лицензия (DreamSpark); 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор) Бесплатное ПО; Adobe Acrobat Reader Бесплатное ПО; Adobe Flash Player Бесплатное ПО; FAR file manager Бесплатное ПО; Google Chrome Бесплатное ПО; Java TM 7 (64-bit)Бесплатное ПО; K-Lite Codec Pack Бесплатное ПО; Mozilla Firefox Бесплатное ПО; Oracle VM VirtualBox Бесплатное ПО; Sublime Text Бесплатное ПО; Symantec*

	технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-Р3.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920	*Endpoint Protection 12 (Заменен на AVP Kaspersky) Бесплатное ПО; VMWare Player Бесплатное ПО; Антивирус "Зоркий глаз" Бесплатное ПО; Lazarus (аналог Delphi) Бесплатное ПО; Smath Studio (аналог Mathcad) Бесплатное ПО; NanoCAD (аналог Autocad) Бесплатное ПО; Gimp (графичский редактор аналог Photoshop) Бесплатное ПО; Avidemax (видео редактор) Бесплатное ПО; Virtual Dub (видео редактор) Бесплатное ПО; Free Pascal Бесплатное ПО (ауд.420) Страж NT вер.3.0 Сертификат ФСТЭК No 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК No 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК No 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК No1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК No3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК No1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК No2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК No2945 16.08.2013*
Аудитории для самостоятельной работы, курсового и дипломного проектирования	*Читальные залы библиотеки: Компьютеры со свободным доступом в сеть Интернет и Электронными библиотечными и информационно справочными системами; Ауд.424: Комплекты мебели для учебного процесса. Количество ПЭВМ – 12 (рабочая станция CPU Core 2Duo E6300 – 1.86 – 10 шт, Celeron D2.8 – 2 шт.), стенды – 3*	

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

8.1 **Оценочные материалы** (ОМ) для дисциплины включают:

- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;
- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

8.2 Для каждого результата обучения по дисциплине определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины**.

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

Документ составлен в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем и специализации Безопасность открытых информационных систем.

АННОТАЦИЯ
К РАБОЧЕЙ ПРОГРАММЕ
ДИСЦИПЛИНЫ
«СИСТЕМА ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК»
(наименование дисциплины)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– способностью проводить анализ защищенности автоматизированных систем (ПК-3);

– способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

– способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);

– способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);

– способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);

– способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

– способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

– способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

– способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

– способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

– способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

В результате освоения дисциплины студент должен:

Знать

– основные задачи администрирования подсистемы ИБ объекта защита; инструменты администрирования;

– описание уязвимостей рассматриваемого объекта или ресурса;

– системы, комплексы и средства обеспечения информационной безопасности;

– основные программные, программно-аппаратные и технические средства защиты информации; основные метрологические показатели средств защиты информации;

– основные нормативные акты сертификации;

– основные средства и способы обеспечения ИБ, принципы построения системы защиты ИБ;

– применять методы и способы защиты информации в информационных системах персональных данных;

– принципы организации информационных систем в соответствии с требованиями по защите информации;

– принципы организации информационных систем в соответствии с требованиями по защите информации;

– подходы к формированию и реализации политики информационной безопасности автоматизированных систем;

– комплекс мероприятий по обеспечению информационной безопасности автоматизированных систем;

Уметь

– проводить анализ угроз безопасности автоматизированных систем;

– использовать методы оценки уязвимости защищаемых персональных данных, построения модели угроз;

– проектировать комплексную систему защиты информации и информационных систем;

– организовывать и проводить контрольные проверки работоспособности средств защиты информации;

– находить и определять область применения различных категорий и видов стандартов, систем стандартов, классификаторов и указателей, документацией продукции, процессов, услуг и систем качества;

– разрабатывать частные политики информационной безопасности информационных систем;

– определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем;

– разрабатывать частные политики информационной безопасности информационных (автоматизированных) систем;

– разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;

– составлять политики информационной безопасности для автоматизированных систем и применять их на практике;

– определять перспективные направления и пути совершенствования автоматизированной системы;

Владеть

– моделями, методами и инструментами многослойной защиты информации;

– методами построения модели угроз и нарушителей;

– методами и средствами проектирования систем обеспечения информационной безопасности и защиты информационных систем;

– методами и инструментами оценки эффективности;

– навыками использования различных категорий и видов стандартов, систем стандартов, классификаторов и указателей, документацией продукции, процессов, услуг и систем качества;

– навыками разработки документирования, тестирования и отладки программного обеспечения по защите информации;

– навыками анализа информационной инфраструктуры информационной системы и ее безопасности;

– профессиональной терминологией в области информационной безопасности;

– навыками выбора и обоснования критериев эффективности функционирования защищенных информационных (автоматизированных) систем;

– навыками составления и использования политик информационной безопасности;

– навыками участия в формировании, организации и поддержки комплекса мер по обеспечению информационной безопасности автоматизированной системы.

Содержание разделов дисциплины. Основные понятия и определения. Уязвимости TCP/IP протокола. Слабости межсетевого экрана, и способы его обхода. Уязвимость аутентификации и авторизации. Основная классификация уязвимостей. Модель атаки. Этапы реализации атак. Классификация атак. Основные признаки атак. Источники информации об атаках. Технологии и подходы к обнаружению. Системы анализа защищённости. Анализаторы журналов регистрации. Обманные системы. Системы контроля целостности. Контроль изменений файлов. Анализ журналов регистрации. Анализ сетевого трафика. Анализ сервисов и портов. Предварительный анализ. Критерии оценки. Тестирование. Обоснование для руководства. Размещение сенсоров. Использование сетевых сенсоров в коммутируемых сетях. Размещение системы анализа защищённости. Размещение системы контроля целостности. Размещение обманной системы. Основные аспекты создания системы обнаружения атак. Общая концепция. Сенсорный блок. Блок анализа. Блок реагирования.