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
Программно-аппаратные средства защиты информации

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

Целью освоения дисциплины «Программно-аппаратные средства защиты информации» является подготовка выпускника к деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, программного обеспечения, предназначенных для обеспечения защиты информации.

Данный курс, на основе использования международных российских стандартов и нормативных требований ФСБ, ФСТЭК и Роскомнадзора России в сфере обеспечения информационной безопасности, вырабатывает у студентов знания о сущности, понятии и способах обеспечения информационной безопасности, принципах построения систем защиты информации, а также умение классифицировать и оценивать угрозы информационной безопасности.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Программно-аппаратные средства защиты информации» относится к числу дисциплин базовой части профессионального цикла. (Б1.О.09)

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

«Аппаратные средства вычислительной техники» - знание основ организации и работы аппаратных компьютерных средств;

«Информатика» – работа с программными средствами общего назначения;

«Основы информационной безопасности» – знание основ обеспечения информационной безопасности в Российской Федерации.

Знания и навыки, полученные в результате изучении дисциплины «Программно-аппаратные средства защиты информации», используются студентами в дальнейшем 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, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	**И-ОПК-10_3** знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности и принципы формирования политики информационной безопасности организации.	**Знать** основные принципы и правовые основы формирования политики безопасности предприятия с учетом рисков и сферой деятельности данного предприятия.
	И-ОПК-10_4 знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	**Знать** программные, программно-аппаратные средства защиты информации в компьютерных системах и сетях (в части операционных систем). **Владеть навыками** администрирования данных средств защиты информации в компьютерных системах и сетях.

	И-ОПК-10_5 умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	**Знать** порядок выполнения работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. **Уметь** выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	**И-ОПК-12.1** знает принципы формирования политики информационной безопасности в информационных системах, принципы организации информационных систем в соответствии с требованиями по защите информации; основные этапы процесса проектирования и общие требования к содержанию проекта;	**Знать** принципы формирования политики информационной безопасности предприятия. **Знать** основы и принципы построения защищенных информационных систем. **Уметь** проектировать защищенные информационные системы с учетом требований к содержанию проекта.

	И-ОПК-12.2 умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;	**Знать** перечень мероприятий и порядок проведения контрольных проверок работоспособности и эффективности программно-аппаратных средств защиты информации. **Уметь** определять информационную инфраструктуру предприятия и его ресурсы, подлежащие защите.
	И-ОПК-12.3 умеет оценивать информационные риски в автоматизированных системах; умеет разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений;	**Знать** методики оценивания информационных рисков в автоматизированных системах (операционных системах и сетях). **Уметь** оценивать уровень безопасности компьютерных систем и сетей и проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные 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	Подсистемы защиты современных операционных систем	6	7	6	7	3		20	Опрос на практических занятиях
2	Защита информации в компьютерных сетях	6	4	4	3			13,7	Опрос на практических занятиях
3	Защита программ и данных	6	5	6	6	1		20	Опрос на практических занятиях
						2	0,3		Зачет
	Всего	108	16	16	16	6	0,3	53,7	

Содержание разделов дисциплины:

Раздел № 1 «Подсистемы защиты современных операционных систем».

Тема 1.1. Субъекты, объекты, методы и права доступа в современных операционных системах.

Тема 1.2. Основные компоненты подсистем защиты UNIX и Windows (управление доступом, аутентификация, аудит).

Тема 1.3. Основные проблемы с безопасностью и возможные решения в современных операционных системах.

Тема 1.4. Аудит информационной безопасности.

Раздел № 2 «Защита информации в компьютерных сетях».

Тема 2.1. Обеспечение безопасности межсетевого взаимодействия.

Тема 2.2. Адаптивная безопасность в вычислительных сетях.

Раздел № 3 «Защита программ и данных».

Тема 3.1. Защита программ от изучения, несанкционированного копирования и использования.

Тема 3.2. Принципы построения политики безопасности, обеспечивающей высокую защищенность от вредоносного программного обеспечения: принцип минимизации программного обеспечения, принцип минимизации полномочий пользователей.

Тема 3.3. Методы и средства обеспечения сохранности информации. Особенности резервирования и восстановления данных в современных условиях.

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.

Практические и лабораторные занятия – занятия, посвященные освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

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 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;
- СЗИ НСД Dallas Lock 8.0-K.;
- Средства защиты информации Secret Net 7;
- Linux (GNU GPL v.3).
- Academic VMware Fusion 10 Pro ESd.
- Academic VMware Workstation 14 Pro for Linux and Windows ESD.
- IDA 5.x (бесплатная версия ПО);
- Microsoft Debugging Tools (свободно распространяемое ПО);
- Virtual Box (GNU GPL v.2).

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

1. Автоматизированная библиотечно-информационная система «БУКИ-NEXT» - https://www.lib.uniyar.ac.ru/opac/bk_cat_find.php/
2. Электронно-библиотечная система «Юрайт - https://www.biblio-online.ru/
3. Электронно-библиотечная система «Лань» - http://e.lanbook.com/

4. Портал разработчиков клиент-серверных приложений Microsoft Developer Network (MSDN) - https://msdn.microsoft.com/ru-ru/

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

а) основная литература

1. Платонов, В.В. «Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей»: учебное пособие для вузов / В. В. Платонов; УМО по образованию в обл. информационной безопасности. - М.: Академия, 2006. - 239 с. - (Высшее проф. образование. Информационная безопасность).
   Режим доступа:
   http://www.lib.uniyar.ac.ru/opac/bk_cat_card.php?rec_id=355769&cat_cd=YARSU
1. Мифтахова, Л. Х. Программно-аппаратные средства защиты информации : учебное пособие / Л. Х. Мифтахова, А. Р. Касимова, В. Н. Красильников, В. А. Богомолов, А. Д. Алехин. - Санкт-петербург : ИЦ Интермедия, 2018. - 408 с. - ISBN 978-5-4383-0157-8. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785438301578.html (дата обращения: 25.01.2022). - Режим доступа : по подписке.
2. Проскурин В.Г., «Защита программ и данных», 2-е издание, учебное пособие для студ. учреждений высш. проф. образования, М., Издательский центр «Академия», 2012.- 208с.
3. Проскурин, В. Г. Защита в операционных системах : учебное пособие для вузов / Проскурин В. Г. - Москва : Горячая линия - Телеком, 2014. - 192 с. - ISBN 978-5-9912-0379-1. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991203791.html (дата обращения: 26.01.2022). - Режим доступа : по подписке.
4. Федеральный закон от 26 июля 2017 года №187 – ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
5. ГОСТ Р ИСО/МЭК 51583 - 2014 года, «Порядок создания автоматизированных систем в защищенном исполнении», Федеральное агентство по техническому регулированию и метрологии («Росстандарт»), М.: 2014.-22с.

б) дополнительная литература

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491249 (дата обращения: 26.01.2022).
2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство

Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493262 (дата обращения: 26.01.2022). Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 424 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52161.html

3. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 26.01.2022). — Режим доступа: для авториз. пользователей.

4. Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. — Электрон. текстовые данные. — Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. — 224 с. — 978-5-9515-0305-3. — Режим доступа: http://www.iprbookshop.ru/60959.html

5. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : учебное пособие для вузов / Под ред. профессора О. И. Шелухина. - Москва : Горячая линия - Телеком, 2013. - 220 с. - ISBN 978-5-9912-0323-4. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991203234.html (дата обращения: 26.01.2022). - Режим доступа : по подписке.

6. Таненбаум Э. Современные операционные системы. / Э. Таненбаум; [пер. с англ. Н. Вильчинского, А. Лашкевича] - 4-е изд. - СПб.: Питер, 2015. - 1115 с.

7. Организация безопасной работы информационных систем [Электронный ресурс] : учебное пособие для студентов, обучающихся по направлению 230400 «Информационные системы и технологии», 230701 «Прикладная информатика» / Ю.Ю. Громов [и др.]. — Электрон. текстовые данные. — Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2014. — 132 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/64142.html

8. ГОСТ 51583 - 2014 года, «Порядок создания автоматизированных систем в защищенном исполнении», Федеральное агентство по техническому регулированию и метрологии («Росстандарт»), М.: 2014.-22с.

9. ГОСТ Р ИСО/МЭК 15408-1-2012г., 15408-2-2013г., 15408-3-2013г., «Информационная технология. Методы и средства обеспечения информационной безопасности. Критерии оценки безопасности информационных технологий», «Часть 1. Введение и общая модель», «Часть 2. Функциональные компоненты безопасности», «Часть. 3. Компоненты доверия к безопасности», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», Часть 1.-2014.-56с., Часть 2.-2014.-164с., Часть 3.-2014.-152с.

10. Национальный стандарт ГОСТ Р ИСО/МЭК 53113-1-2008 «Информационные технологии. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов. Часть 1. Общие положения».

11. Национальный стандарт 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».

12. Руководящий документ ФСТЭК России (бывш. Гостехкомиссия) «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств

защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей». (утв. решением Государственной технической комиссии при Президенте РФ от 4 июня 1999 г., № 114).

9. 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 и практических занятий (семинаров);
- лаборатория программно-аппаратных средств обеспечения информационной безопасности;
- лаборатория технической защиты информации;
- 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.

Автор:
Ассистент кафедры КБ и ММОИ. К. Ю. Герасимова

Приложение №1 к рабочей программе дисциплины
«Программно-аппаратные средства защиты информации»

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

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Перечень вопросов для опросов на практических занятиях:

1. Управление доступом в UNIX.
2. Базовые средства управления доступом в Windows: маркеры доступа, дескрипторы защиты.
3. Назначение атрибутов защиты вновь создаваемым объектам Windows, наследование дескрипторов защиты.
4. Управление средствами аутентификации в Linux.
5. Управление средствами аутентификации в Windows.
6. Управление средствами аудита в Linux.
7. Управление средствами аудита в Windows.
8. Управление доменами Windows.
9. Нападения на политику безопасности и процедуры административного управления.
10. Нападения на постоянные компоненты системы защиты.
11. Нападения на функциональные элементы компьютерных сетей.
12. Нападения на протоколы информационного взаимодействия.
13. Безопасность удаленного доступа к локальной сети.
14. Централизованный контроль удаленного доступа.
15. Организация безопасного удаленного доступа.
16. Противодействие несанкционированному межсетевому доступу.
17. Аутентификация удаленных пользователей.
18. Разработка политики межсетевого взаимодействия.
19. Основные принципы построения политики безопасности, повышающей защищенность от вредоносного программного обеспечения.
20. На основе учебной литературы и положений национального стандарта ГОСТ Р ИСО/МЭК 51583-2014 «Порядок создания автоматизированных систем в защищенном исполнении», обобщите и сформулируйте порядок и этапы построения защищенных информационных систем на основе защищенных баз данных.
21. Приведите номера и названия нескольких основных правовых нормативных документов в сфере информационной безопасности, регламентирующих проведение работ по администрированию средств защиты информации в компьютерных системах и сетях.
22. Кратко расскажите о порядке проведения работ по администрированию средств защиты информации в компьютерных системах и сетях, предусмотренном действующими правовыми нормативными документами в сфере информационной безопасности.
23. Приведите номера и названия нескольких основных правовых нормативных документов в сфере информационной безопасности, регламентирующих администрированию системного программного обеспечения в компьютерных системах и сетях.

24. Кратко расскажите о содержании работ по администрированию системного программного обеспечения в компьютерных системах и сетях, предусмотренных действующими правовыми нормативными документами в сфере информационной безопасности.

25. Кратко расскажите о методике оценивания уровня безопасности компьютерных систем и сетей, предусмотренной действующими правовыми нормативными документами в сфере информационной безопасности. Приведите номера и названия этих документов.

26. Кратко расскажите о методике проведения экспериментальных исследований компьютерных систем с целью выявления уязвимостей, предусмотренной действующими правовыми нормативными документами в сфере информационной безопасности. Приведите номера и названия этих документов.

27. Кратко расскажите о методике проведения контрольных проверок работоспособности и эффективности, применяемых программно-аппаратных и технических средств защиты информации, предусмотренной действующими правовыми нормативными документами в сфере информационной безопасности. Приведите номера и названия этих документов.

28. Кратко расскажите о методике организации и сопровождении аттестации объектов информатизации по требованиям безопасности информации, предусмотренной действующими правовыми нормативными документами в данной сфере. Приведите номера и названия этих документов.

29. Кратко расскажите о методике (порядке и содержании) проведения установки, настройки и обслуживании программно-аппаратных (в том числе и криптографических) технических средств защиты информации, предусмотренной действующими правовыми нормативными документами в сфере информационной безопасности. Приведите номера и названия этих документов.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к зачету:

На зачете проверяется сформированность компетенций ОПК-10; ОПК-12 (подробнее в п. 3).

1. Типовая архитектура подсистемы безопасности защищенной ОС.
2. Средства администрирования в защищенной ОС (система управления списком пользователей и политикой безопасности, менеджер ресурсов, аудит, сервисы)
3. Методы и права доступа в ОС Windows.
4. Порядок проверки прав доступа субъекта к объектам в ОС Windows.
5. Методы проверки прав доступа субъекта к объекту семейства ОС Unix.
6. Атрибуты защиты и векторы доступа семейства ОС Unix.
7. Механизм SUID/SGID семейства ОС Unix.
8. Парольная аутентификация. Ее «плюсы» и «минусы».
9. Аутентификация с использованием внешних носителей.
10. Биометрическая аутентификация.
11. Аутентификация в UNIX.
12. Аутентификация в Windows.
13. Общие сведения по аудиту защищенных ОС.
14. Проблемы обеспечения безопасности при удалённом доступе к сети.
15. Организация безопасного удаленного доступа. Обзор протоколов аутентификации при удалённом доступе.
16. Спецификации протокола PPP.

17. Протоколы аутентификации PAP и CHAP. Основные принципы функционирования и использования протокола PPTP.
18. Протокол PAP.
19. Протокол S/Key.
20. Протокол CHAP.
21. Централизованный контроль удаленного доступа.
22. Основные принципы функционирования и использования протоколов TACACS и RADIUS. Обзор систем серверов TACACS и RADIUS и их функциональных возможностей.
23. Протокол Керберос, как универсальный инструмент надежной авторизации в сетях установления доверительных отношений, независимо от типа ОС.
24. Техническая защита от несанкционированного копирования. Подсистема противодействия нейтрализации защитных механизмов.
25. Привязка программ к аппаратным средствам. Идентификация параметров аппаратной платформы, жестких дисков, оценка уникальности параметров компьютера.
26. Базовые методы нейтрализации систем защиты от несанкционированного копирования.
27. Роль файловых систем ОС Microsoft и Linux для защиты программ и данных.
28. Принципы построения политики безопасности, обеспечивающей высокую защищенность от вредоносного программного обеспечения.
29. Принцип минимизации программного обеспечения.
30. Принцип минимизации полномочий пользователей.
31. Методы и средства обеспечения сохранности информации.
32. Особенности резервирования и восстановления данных в современных условиях

Правила выставления оценки на зачете.

В билет включается два теоретических вопроса. На подготовку к ответу дается не менее 40 минут.

По итогам зачета выставляется одна из оценок: «зачтено», «не зачтено».

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. Продвинутый уровень превосходит 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.

Оценка «**зачтено**» 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 (например, студент не владеет терминологией и не знает основных определений и понятий в проверяемом разделе).

Оценка «**не зачтено**» выставляется также студенту, который взял билет, но отвечать отказался.

Приложение № 2 к рабочей программе дисциплины
«Программно-аппаратные средства защиты информации»

Методические указания для студентов по освоению дисциплины

Основной учебного материала по дисциплине «Программно-аппаратные средства защиты информации» являются лекции и источники основной и дополнительной литературы, вместе с Web-материалами, указанными в Рабочей программе и доведенными до студентов (преподавателем и через возможности библиотечного фонда ЯрГУ). Данная дисциплина является логичным продолжением курсов: «Аппаратные средства вычислительной техники» и «Основы информационной безопасности».

Для успешного освоения дисциплины важно углубленное самостоятельное изучение всех тем дисциплины упомянутых в рекомендуемых источниках. Наибольшего эффекта можно достичь с помощью упреждающего ознакомления с материалом по темам занятий из источников литературы, после чего на лекциях и практических занятиях преподавателями до студентов доводится критический анализ имеющихся документов, подходов и алгоритмов решений в сфере обеспечения информационной безопасности в России, порой не соответствующих ни реалиям жизни, ни быстро меняющейся международной обстановке, ни изменениям в нормативной базе.

Также, в процессе изучения дисциплины, рекомендуется регулярное повторение пройденного на лекциях и практических занятиях материала. Материал, законспектированный на лекциях и представленный в учебной литературе, необходимо еще раз после занятий прорабатывать и, при необходимости, дополнять актуальной информацией, полученной из рекомендованных ресурсов сети «Интернет», на практических и лабораторных занятиях.

Для проверки и контроля усвоения теоретического материала, приобретенных практических, проводятся мероприятия текущей аттестации в виде опросов на практических занятиях и учитываются, на ряду с результатами практических занятий, при оценке текущей успеваемости. Также проводятся консультации (при необходимости) по разбору наиболее сложных для усвоения тем, которые вызвали затруднения у студентов.

В конце изучения дисциплины студенты сдают зачет. Зачет принимается по билетам, каждый из которых включает в себя два теоретических вопроса. На самостоятельную подготовку к зачету выделяется 3 дня, предусмотрены групповые консультации.