МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Институт компьютерных наук и технологий

Авторы-составители: **Черников Арсений Викторович**
Айдаров Юрий Рафаэлевич
Мустакимова Яна Романовна
Неверов Алексей Валерьевич

Рабочая программа дисциплины

АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Код УМК 93161

Утверждено
Протокол №6
от «06» мая 2022 г.

Пермь, 2022

1. Наименование дисциплины

Анализ уязвимостей программного обеспечения

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.01** Компьютерная безопасность

направленность Разработка защищенного программного обеспечения

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Анализ уязвимостей программного обеспечения** у обучающегося должны быть сформированы следующие компетенции:

10.05.01 Компьютерная безопасность (направленность : Разработка защищенного программного обеспечения)

ОПК.13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности

Индикаторы

ОПК.13.1 Применяет теоретические знания информационной безопасности и программирования для разработки компонент программно-аппаратных средств защиты информации

ОПК.13.2 Проводит анализ безопасности компьютерных систем при применении разработанных компонент программно-аппаратных средств защиты информации

ПК.1 Способен проводить анализ защищенности компьютерных систем и сетей

Индикаторы

ПК.1.1 Ориентируется в методах и средствах анализа защищенности компьютерных систем и сетей

ПК.1.2 Выбирает необходимые для решения профессиональной задачи методы и средства анализа защищенности компьютерных систем и сетей

ПК.1.3 Применяет методы и средства мониторинга и анализа защищенности компьютерных систем и сетей

ОПСК.1 Способен проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей

Индикаторы

ОПСК.1.1 Ориентируется в требованиях нормативных документов по разработке программного кода

ОПСК.1.2 Выполняет тестирование программного кода

ОПСК.1.3 Применяет на практике методы и средства анализа программного кода

ОПСК.1.4 Осуществляет поиск потенциальных уязвимостей и недокументированных возможностей программного кода

4. Объем и содержание дисциплины

Специальность	10.05.01 Компьютерная безопасность (направленность: Разработка защищенного программного обеспечения)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	16
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	42
Проведение лекционных занятий	14
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Защищаемое контрольное мероприятие (2) Письменное контрольное мероприятие (1)
Формы промежуточной аттестации	Зачет (16 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Понятие и классификация уязвимостей программного обеспечения

Понятие уязвимости программного обеспечения (ПО). Уязвимость ПО как угроза информационной безопасности. Источники учзвимостей. Классификация уязвимостей. Методы борьбы с уязвимостями. Предотвращение уязвимостей на этапе разработки ПО. Обнаружение уязвимостей. Анализ уязвимостей: цели, задачи и методы. Способы устранения уязвимостей. Неустранимые уязвимости и методы противодействия им.

Уязвимости этапа проектирования программного обеспечения

Уязвимости этапа проектирования ПО: ошибки, логические и алгоритмические ошибки. Технологические приемы минимизации уязвимостей на этапе проектирования ПО.

Разработка безопасного программного обеспечения

Предотвращение уязвимостей на этапе реализации

Уязвимости этапа реализации: ошибки и программные закладки. Типовые уязвимости ПО, возникающие на этапе реализации. Понятие безопасного кодирования. Технологические приемы безопасного кодирования. Средства языков и сред программирования, способствующих минимизации количества уязвимостей.

Исключения и конструкции обработки исключений. Управление входными данными. Контроль памяти: массивы, списочные структуры, динамическое выделение памяти. Утечка памяти как уязвимость. Потенциальные уязвимости многопоточных программ. Специфические уязвимости баз данных и программ, взаимодействующих с ними. Логирование работы ПО. Специфические уязвимости web-сервисов.

Безопасное использование сторонних библиотек. Паттерны как средство минимизации количества потенциальных уязвимостей.

Методы анализа ПО и его уязвимостей. Тестирование как средство обнаружения уязвимостей.

Стандарты, требования и рекомендации по разработке безопасного ПО и минимизации уязвимостей ПО

Стандарты в области разработки безопасного ПО. ГОСТ Р 56939-2016.

Актуальные уязвимости современного программного обеспечения

Уязвимости web-сервисов. Потенциальные уязвимости современных браузеров и фреймворков.

Уязвимости мобильных приложений.

Уязвимости серверов баз данных.

Уязвимости облачных технологий.

Итоговое контрольное мероприятие

Проводится в виде комплексного теста по дисциплине.

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Аблязов, Р. З. Программирование на ассемблере на платформе x86-64 / Р. З. Аблязов. — 2-е изд. — Саратов : Профобразование, 2019. — 301 c. — ISBN 978-5-4488-0117-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/88005

2. Введение в разработку приложений для ОС Android : учебное пособие / Ю. В. Березовская, О. А. Юфрякова, В. Г. Вологдина [и др.]. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 427 c. — ISBN 978-5-4497-0890-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/102000

3. Баранов, Р. Д. Практические аспекты разработки веб-ресурсов : учебное пособие / Р. Д. Баранов, С. А. Иноземцева, А. А. Рябова. — Саратов : Вузовское образование, 2018. — 121 c. — ISBN 978-5-4487-0263-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/75692.html

Дополнительная:

1. Амоа, К. А. Разработка программных пакетов на языке Python : учебное пособие / К. А. Амоа, Н. А. Рындин, Ю. С. Скворцов. — Воронеж : Воронежский государственный технический университет, ЭБС АСВ, 2020. — 61 c. — ISBN 978-5-7731-0887-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. https://www.iprbookshop.ru/108184

2. Семакова, А. Введение в разработку приложений для смартфонов на ОС Android : учебное пособие / А. Семакова. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 102 c. — ISBN 978-5-4497-0892-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/102001

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

http://www.psu.ru/elektronnye-resursy-dlya-psu Электронные ресурсы для ПГНИУ
http://www.mathnet.ru/ Общероссийский математический портал
http://window.edu.ru/ Единое окно доступа к образовательным ресурсам
https://www.kb.cert.org/vuls/ База данных уязвимостей ПО института SEI

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Анализ уязвимостей программного обеспечения** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине "Анализ уязвимостей программного обеспечения" предполагает использование следующего программного обеспечения и информационных справочных систем:
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета.

Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:
- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Adobe Acrobat Reader DC»;
- офисный пакет приложений «LibreOffice».

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (student.psu.ru).
1. HEX-редактор
2. Дизассемблер

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

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

Для лекционных занятий требуется аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для лабораторных работ требуется аудитория Лаборатории Информационной безопасности: аппаратные и программные средства определены паспортом лаборатории.
Для групповых (индивидуальных) консультаций - аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.

Для проведения текущего контроля - аудитория, оснащенная меловой (и) или маркерной доской. Самостоятельная работа студентов: аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», с обеспеченным доступом в электронную информационно-образовательную среду университета, помещения Научной библиотеки ПГНИУ.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.
5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Анализ уязвимостей программного обеспечения

Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания

ОПК.13

Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.13.1 Применяет теоретические знания информационной безопасности и программирования для разработки компонент программно-аппаратных средств защиты информации	Знать теоретические основы информационной безопасности и теоретические основы безопасного программирования. Уметь применять теоретические знания информационной безопасности и теоретические основы безопасного программирования для решения практических задач. Владеть методами и технологиями безопасного программирования для разработки компонент программно-аппаратных средств защиты информации.	**Неудовлетворител** Не знает теоретические основы информационной безопасности и теоретические основы безопасного программирования. Не умеет применять теоретические знания информационной безопасности и теоретические основы безопасного программирования для решения практических задач. Не владеет методами и технологиями безопасного программирования для разработки компонент программно-аппаратных средств защиты информации. **Удовлетворительн** Знает теоретические основы информационной безопасности и теоретические основы безопасного программирования. Фрагментарно умеет применять теоретические знания информационной безопасности и теоретические основы безопасного программирования для решения практических задач. Не владеет методами и технологиями безопасного программирования для разработки компонент программно-аппаратных средств защиты информации. **Хорошо** Знает теоретические основы информационной безопасности и теоретические основы безопасного программирования. Умеет применять теоретические знания информационной безопасности и теоретические основы безопасного

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо программирования для решения практических задач. Владеет не в полной мере методами и технологиями безопасного программирования для разработки компонент программно-аппаратных средств защиты информации. **Отлично** Знает теоретические основы информационной безопасности и теоретические основы безопасного программирования. Умеет применять теоретические знания информационной безопасности и теоретические основы безопасного программирования для решения практических задач. Владеет в полной мере методами и технологиями безопасного программирования для разработки компонент программно-аппаратных средств защиты информации.
ОПК.13.2 Проводит анализ безопасности компьютерных систем при применении разработанных компонент программно-аппаратных средств защиты информации	Знать основные требования к безопасности компьютерных систем и их отдельных компонент. Уметь анализировать безопасность компьютерных систем при применении разработанных компонент программно-аппаратных средств защиты информации. Владеть методами анализа и оценки безопасности компьютерных систем при внедрении в них программно-аппаратных средств защиты информации.	**Неудовлетворител** Не знает основные требования к безопасности компьютерных систем и их отдельных компонент. Не умеет анализировать безопасность компьютерных систем при применении разработанных компонент программно-аппаратных средств защиты информации. Не владеет методами анализа и оценки безопасности компьютерных систем при внедрении в них программно-аппаратных средств защиты информации. **Удовлетворительн** Фрагментарно знает основные требования к безопасности компьютерных систем и их отдельных компонент. Умеет выборочно анализировать безопасность компьютерных систем при применении разработанных компонент программно-аппаратных средств защиты информации. Не владеет методами анализа и оценки

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн безопасности компьютерных систем при внедрении в них программно-аппаратных средств защиты информации. **Хорошо** Знает все основные требования к безопасности компьютерных систем и их отдельных компонент. Умеет полностью анализировать безопасность компьютерных систем при применении разработанных компонент программно-аппаратных средств защиты информации. Владеет не в полной мере методами анализа и оценки безопасности компьютерных систем при внедрении в них программно-аппаратных средств защиты информации. **Отлично** Знает все основные требования к безопасности компьютерных систем и их отдельных компонент. Умеет полностью анализировать безопасность компьютерных систем при применении разработанных компонент программно-аппаратных средств защиты информации. Владеет в полной мере методами анализа и оценки безопасности компьютерных систем при внедрении в них программно-аппаратных средств защиты информации.

ОПСК.1

Способен проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПСК.1.1 Ориентируется в требованиях нормативных документов по разработке программного кода	Знать основные требования нормативных документов по разработке защищенного программного кода. Уметь применять требования нормативных документов по разработке защищенного программного кода при решении профессиональных	**Неудовлетворител** Не знает основные требования нормативных документов по разработке защищенного программного кода. Не умеет обосновывать выбор требований нормативных документов по разработке защищенного программного кода при решении профессиональных задач. Не владеет навыками поиска необходимой

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
	задач. Владеть навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода.	**Неудовлетворител** информации в нормативных документах по разработке защищенного программного кода. **Удовлетворительн** Знает не все основные требования нормативных документов по разработке защищенного программного кода. Плохо умеет обосновывать выбор требований нормативных документов по разработке защищенного программного кода при решении профессиональных задач. Не владеет навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода. **Хорошо** Знает все основные требования нормативных документов по разработке защищенного программного кода. Хорошо умеет обосновывать выбор требований нормативных документов по разработке защищенного программного кода при решении профессиональных задач. Не в полной мере владеет навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода. **Отлично** Знает все основные требования нормативных документов по разработке защищенного программного кода. Хорошо умеет обосновывать выбор требований нормативных документов по разработке защищенного программного кода при решении профессиональных задач. В полной мере владеет навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода.
ОПСК.1.2 Выполняет тестирование программного кода	Знать основные методы тестирования программного кода. Уметь применять методы тестирования программного	**Неудовлетворител** Не знает основные методы тестирования программного кода. Не умеет применять методы тестирования программного кода.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
	кода. Владеть навыками тестирования программного кода при решении профессиональных задач.	**Неудовлетворител** Не владеет навыками тестирования программного кода при решении профессиональных задач. **Удовлетворительн** Знает основные методы тестирования программного кода. Не умеет применять методы тестирования программного кода. Не владеет навыками тестирования программного кода при решении профессиональных задач. **Хорошо** Знает основные методы тестирования программного кода. Умеет применять методы тестирования программного кода. Владеет не в полной мере навыками тестирования программного кода при решении профессиональных задач. **Отлично** Знает основные методы тестирования программного кода. Умеет применять методы тестирования программного кода. Владеет в полной мере навыками тестирования программного кода при решении профессиональных задач.
ОПСК.1.3 Применяет на практике методы и средства анализа программного кода	Знать основные методы и средства анализа программного кода. Уметь применять основные методы и средства анализа программного кода. Владеть навыками применения методов и средств анализа программного кода при решении профессиональных задач.	**Неудовлетворител** Не знает основные методы и средства анализа программного кода. Не умеет применять основные методы и средства анализа программного кода. Не владеет навыками применения методов и средств анализа программного кода при решении профессиональных задач. **Удовлетворительн** Знает основные методы и средства анализа программного кода. Не умеет применять основные методы и средства анализа программного кода. Не владеет навыками применения методов и средств анализа программного кода при решении профессиональных задач. **Хорошо**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо Знает основные методы и средства анализа программного кода. Умеет применять основные методы и средства анализа программного кода. Владеет не в полной мере навыками применения методов и средств анализа программного кода при решении профессиональных задач. **Отлично** Знает основные методы и средства анализа программного кода. Умеет применять основные методы и средства анализа программного кода. Владеет в полной мере навыками применения методов и средств анализа программного кода при решении профессиональных задач.
ОПСК.1.4 Осуществляет поиск потенциальных уязвимостей и недокументированных возможностей программного кода	Знать основные уязвимости и недокументированные возможности программного кода. Уметь проверять программный код на наличие потенциальных уязвимостей и недокументированных возможностей. Владеет методами поиска потенциальных уязвимостей и недокументированных возможностей программного кода.	**Неудовлетворител** Не знает основные уязвимости и недокументированные возможности программного кода. Не умеет проверять программный код на наличие потенциальных уязвимостей и недокументированных возможностей. Не владеет методами поиска потенциальных уязвимостей и недокументированных возможностей программного кода. **Удовлетворительн** Знает основные уязвимости и недокументированные возможности программного кода. Частично умеет проверять программный код на наличие потенциальных уязвимостей и недокументированных возможностей. Не владеет методами поиска потенциальных уязвимостей и недокументированных возможностей программного кода. **Хорошо** Знает основные уязвимости и недокументированные возможности программного кода. Полностью умеет проверять программный код на наличие потенциальных уязвимостей и недокументированных возможностей.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо Владеет не в полной мере методами поиска потенциальных уязвимостей и недокументированных возможностей программного кода. **Отлично** Знает основные уязвимости и недокументированные возможности программного кода. Полностью умеет проверять программный код на наличие потенциальных уязвимостей и недокументированных возможностей. Владеет в полной мере методами поиска потенциальных уязвимостей и недокументированных возможностей программного кода.

ПК.1

Способен проводить анализ защищенности компьютерных систем и сетей

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.1.1 Ориентируется в методах и средствах анализа защищенности компьютерных систем и сетей	Знать основные требования к безопасности компьютерных систем и сетей. Уметь анализировать защищенность компьютерных систем и сетей. Владеть методами и средствами анализа и оценки безопасности компьютерных систем и сетей.	**Неудовлетворител** Не знает основные требования к безопасности компьютерных систем и сетей. Не умеет анализировать защищенность компьютерных систем и сетей. Не владеет методами и средствами анализа и оценки безопасности компьютерных систем и сетей. **Удовлетворительн** Частично знает основные требования к безопасности компьютерных систем и сетей. Частично умеет анализировать защищенность компьютерных систем и сетей. Не владеет методами и средствами анализа и оценки безопасности компьютерных систем и сетей. **Хорошо** Знает все основные требования к безопасности компьютерных систем и сетей. Умеет полностью анализировать защищенность компьютерных систем и сетей. Владеет не в полной мере методами и

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо средствами анализа и оценки безопасности компьютерных систем и сетей. **Отлично** Знает все основные требования к безопасности компьютерных систем и сетей. Умеет полностью анализировать защищенность компьютерных систем и сетей. Владеет в полной мере методами и средствами анализа и оценки безопасности компьютерных систем и сетей.
ПК.1.2 Выбирает необходимые для решения профессиональной задачи методы и средства анализа защищенности компьютерных систем и сетей	Знать основные требования к безопасности компьютерных систем и сетей. Уметь выбирать необходимые для решения профессиональной задачи методы и средства анализа защищенности компьютерных систем и сетей. Владеть методами и средствами анализа и оценки безопасности компьютерных систем и сетей при решении профессиональной задачи.	**Неудовлетворител** Не знает основные требования к безопасности компьютерных систем и сетей. Не умеет выбирать необходимые для решения профессиональной задачи методы и средства анализа защищенности компьютерных систем и сетей. Не владеет методами и средствами анализа и оценки безопасности компьютерных систем и сетей при решении профессиональной задачи. **Удовлетворительн** Знает основные требования к безопасности компьютерных систем и сетей. Умеет не в полной мере выбирать необходимые для решения профессиональной задачи методы и средства анализа защищенности компьютерных систем и сетей. Не владеет методами и средствами анализа и оценки безопасности компьютерных систем и сетей при решении профессиональной задачи. **Хорошо** Знает основные требования к безопасности компьютерных систем и сетей. Умеет в полной мере выбирать необходимые для решения профессиональной задачи методы и средства анализа защищенности компьютерных систем и сетей. Владеет не в полной мере методами и средствами анализа и оценки безопасности компьютерных систем и сетей при решении

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо профессиональной задачи. **Отлично** Знает основные требования к безопасности компьютерных систем и сетей. Умеет в полной мере выбирать необходимые для решения профессиональной задачи методы и средства анализа защищенности компьютерных систем и сетей. Владеет в полной мере методами и средствами анализа и оценки безопасности компьютерных систем и сетей при решении профессиональной задачи.
ПК.1.3 Применяет методы и средства мониторинга и анализа защищенности компьютерных систем и сетей	Знать основные требования к безопасности компьютерных систем и сетей. Уметь применять существующие средства мониторинга и анализа защищенности компьютерных систем и сетей. Владеть методами мониторинга, анализа и оценки защищенности компьютерных систем и сетей.	**Неудовлетворител** Не знает основные требования к безопасности компьютерных систем и сетей. Не умеет применять существующие средства мониторинга и анализа защищенности компьютерных систем и сетей. Не владеет методами мониторинга, анализа и оценки защищенности компьютерных систем и сетей. **Удовлетворительн** Знает основные требования к безопасности компьютерных систем и сетей. Умеет не в полной мере применять существующие средства мониторинга и анализа защищенности компьютерных систем и сетей. Не владеет методами мониторинга, анализа и оценки защищенности компьютерных систем и сетей. **Хорошо** Знает основные требования к безопасности компьютерных систем и сетей. Умеет в полной мере применять существующие средства мониторинга и анализа защищенности компьютерных систем и сетей. Частично владеет методами мониторинга, анализа и оценки защищенности компьютерных систем и сетей. **Отлично** Знает основные требования к безопасности компьютерных систем и сетей.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Умеет в полной мере применять существующие средства мониторинга и анализа защищенности компьютерных систем и сетей. Владеет в полной мере методами мониторинга, анализа и оценки защищенности компьютерных систем и сетей.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Зачет
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 45 до 60
«неудовлетворительно» / «незачтено» менее 45 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПСК.1.2 Выполняет тестирование программного кода **ОПК.13.1** Применяет теоретические знания информационной безопасности и программирования для разработки компонент программно-аппаратных средств защиты информации **ОПК.13.2** Проводит анализ безопасности компьютерных систем при применении разработанных компонент программно-аппаратных средств защиты информации	Предотвращение уязвимостей на этапе реализации **Защищаемое контрольное мероприятие**	Умеет предотвращать появление уязвимостей различного уровня на этапе разработки программ.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПСК.1.4 Осуществляет поиск потенциальных уязвимостей и недокументированных возможностей программного кода **ОПСК.1.3** Применяет на практике методы и средства анализа программного кода **ПК.1.3** Применяет методы и средства мониторинга и анализа защищенности компьютерных систем и сетей **ПК.1.2** Выбирает необходимые для решения профессиональной задачи методы и средства анализа защищенности компьютерных систем и сетей **ПК.1.1** Ориентируется в методах и средствах анализа защищенности компьютерных систем и сетей	Актуальные уязвимости современного программного обеспечения **Защищаемое контрольное мероприятие**	Умеет находить уязвимости в современном ПО.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПСК.1.4 Осуществляет поиск потенциальных уязвимостей и недокументированных возможностей программного кода **ПК.1.2** Выбирает необходимые для решения профессиональной задачи методы и средства анализа защищенности компьютерных систем и сетей **ОПСК.1.2** Выполняет тестирование программного кода **ОПСК.1.1** Ориентируется в требованиях нормативных документов по разработке программного кода **ПК.1.3** Применяет методы и средства мониторинга и анализа защищенности компьютерных систем и сетей **ОПСК.1.3** Применяет на практике методы и средства анализа программного кода **ПК.1.1** Ориентируется в методах и средствах анализа защищенности компьютерных систем и сетей **ОПК.13.2** Проводит анализ безопасности компьютерных систем при применении разработанных компонент программно-аппаратных средств защиты информации **ОПК.13.1** Применяет теоретические знания информационной безопасности и программирования для	Итоговое контрольное мероприятие **Письменное контрольное мероприятие**	Умеет решать задачи пройденного курса.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
разработки компонент программно-аппаратных средств защиты информации		

Спецификация мероприятий текущего контроля

Предотвращение уязвимостей на этапе реализации

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **18**

Показатели оценивания	Баллы
Разработка программы в соотвествие с требованиями к разработке безопасного ПО	30
Анализ и оценка программ соучеников на соотвествие требованиям к разработке безопасного ПО	10

Актуальные уязвимости современного программного обеспечения

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **18**

Показатели оценивания	Баллы
Анализ ПО соучеников, поиск уязвимостей в разработанном ими ПО	20
Разработка web-портала с использованием современных технолоний и в соответствие с требованиями к минимизации уязвимостей	20

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **9**

Показатели оценивания	Баллы
Ответы на вопросы	20