

МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности и систем связи

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 «26» июня 2020 г.

Пермь, 2020

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
специализация 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 (специализация : Разработка защищенного программного обеспечения)

ПК.1 Способность взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий

ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

ПК.11 способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи

ПК.13 способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей

ПК.23 Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами

ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности

ПК.4 способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности

ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований

ПК.9 Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем

ПСК.2 способность проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей

ПСК.5 способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах

ПСК.6 Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности

4. Объем и содержание дисциплины

Направления подготовки	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 уязвимостей. Классификация уязвимостей. Методы борьбы с уязвимостями. Предотвращение уязвимостей на этапе разработки ПО. Обнаружение уязвимостей. Анализ уязвимостей: цели, задачи и методы. Способы устранения уязвимостей. Неустраняемые 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 аудиторские 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 с. — 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. Вологодина [и др.]. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 427 с. — 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 с. — ISBN 978-5-4487-0263-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/75692.html>

Дополнительная:

1. 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 с. — 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-образовательную 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**

ПК.1

Способность взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.1 Способность взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий</p>	<p>Знать способы взаимодействия и сотрудничества с профессиональными сетевыми сообществами. Уметь взаимодействовать и сотрудничать с профессиональными сетевыми сообществами. Уметь отслеживать динамику развития выбранных направлений области информационных технологий.</p>	<p align="center">Неудовлетворител Не умеет взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий.</p> <p align="center">Удовлетворительн Умеет с большими затруднениями взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий.</p> <p align="center">Хорошо Умеет с небольшими затруднениями взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий.</p> <p align="center">Отлично Умеет без затруднений взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий.</p>

ПК.3

Способность к анализу и формализации поставленных задач в области информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.3 Способность к анализу и формализации</p>	<p>Знать методы анализа и формализации поставленных задач.</p>	<p align="center">Неудовлетворител Не умеет анализировать и формализовать поставленные задачи в области</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
поставленных задач в области информационной безопасности	Уметь анализировать и формализовать поставленные задачи в области информационной безопасности. Владеть методами анализа и формализации поставленных задач в области информационной безопасности.	<p>Неудовлетворител информационной безопасности.</p> <p>Удовлетворительн Умеет с большими затруднениями анализировать и формализовать поставленные задачи в области информационной безопасности.</p> <p>Хорошо Умеет с небольшими затруднениями анализировать и формализовать поставленные задачи в области информационной безопасности.</p> <p>Отлично Умеет без затруднений анализировать и формализовать поставленные задачи в области информационной безопасности.</p>

ПК.13

способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.13 способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей	Знать этапы экспериментальных исследований. Уметь проводить экспериментальные исследования компьютерных систем с целью выявления уязвимостей. Владеть методами поиска уязвимостей в компьютерных системах.	<p>Неудовлетворител Не умеет проводить экспериментальные исследования компьютерных систем с целью выявления уязвимостей.</p> <p>Удовлетворительн Умеет с большими затруднениями проводить экспериментальные исследования компьютерных систем с целью выявления уязвимостей.</p> <p>Хорошо Умеет с небольшими затруднениями проводить экспериментальные исследования компьютерных систем с целью выявления уязвимостей.</p> <p>Отлично Умеет без затруднений проводить экспериментальные исследования компьютерных систем с целью выявления уязвимостей.</p>

ПК.23

Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.23 Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	Знать способы защиты информации. Уметь организовать защиту информации техническими и программными средствами. Владеть навыками работы с антивирусным программным обеспечением при работе с компьютерными системами.	Неудовлетворител Не умеет организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами. Удовлетворительн Умеет с большими затруднениями организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами. Хорошо Умеет с небольшими затруднениями организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами. Отлично Умеет без затруднений организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами.

ПК.11

способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.11 способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи	Знать механизмы обеспечения безопасности. Уметь оценивать степень надежности механизмов обеспечения безопасности. Владеть методами оценки степени надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи.	Неудовлетворител Не умеет оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи. Удовлетворительн Умеет с большими затруднениями оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи. Хорошо Умеет с небольшими затруднениями

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Хорошо</p> <p>оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи</p> <p style="text-align: center;">Отлично</p> <p>Умеет без затруднения оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи</p>

ПК.7

Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований</p>	<p>Знать основы информационной безопасности. Уметь провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований</p>	<p style="text-align: center;">Неудовлетворител</p> <p>Не умеет проводить обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований.</p> <p style="text-align: center;">Удовлетворительн</p> <p>Умеет с большими затруднениями проводить обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований.</p> <p style="text-align: center;">Хорошо</p> <p>Умеет с небольшими затруднениями проводить обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований.</p> <p style="text-align: center;">Отлично</p> <p>Умеет без затруднений проводить обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований.</p>

ПК.4

способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.4 способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности	Знать отечественные и зарубежные стандарты в области компьютерной безопасности. Уметь проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности.	Неудовлетворительн Не умеет проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности. Удовлетворительн Умеет с большими затруднениями проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности. Хорошо Умеет с небольшими затруднениями проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности. Отлично Умеет без затруднений проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности.

ПК.9

Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.9 Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем	Знать основы информационной безопасности компьютерных систем. Уметь проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем. Владеть методами анализа проектных решений по обеспечению информационной безопасности компьютерных систем.	Неудовлетворительн Не умеет проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем. Удовлетворительн Умеет с большими затруднениями проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем. Хорошо Умеет с небольшими затруднениями проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Хорошо</p> <p>компьютерных систем.</p> <p style="text-align: center;">Отлично</p> <p>Умеет без затруднений проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем.</p>

ПК.10

Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p>	<p>Знать основы разработки систем защиты информации, формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах. Уметь принимать участие в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p>	<p style="text-align: center;">Неудовлетворител</p> <p>Не умеет участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах.</p> <p style="text-align: center;">Удовлетворительн</p> <p>Умеет с большими трудностями участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах.</p> <p style="text-align: center;">Хорошо</p> <p>Умеет с небольшими затруднениями участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах.</p> <p style="text-align: center;">Отлично</p> <p>Умеет без затруднений участвовать в</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p align="center">Отлично</p> <p>разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах.</p>

ПСК.5

способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПСК.5 способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах</p>	<p>Знать новые образцы программных средств защиты в компьютерных системах. Уметь оценивать эффективность новых образцов программных средств защиты в компьютерных системах. Владеть методами оценки эффективности новых образцов программных средств защиты в компьютерных системах.</p>	<p align="center">Неудовлетворител</p> <p>Не умеет оценивать эффективность новых образцов программных средств защиты в компьютерных системах.</p> <p align="center">Удовлетворительн</p> <p>Умеет с большими затруднениями оценивать эффективность новых образцов программных средств защиты в компьютерных системах.</p> <p align="center">Хорошо</p> <p>Умеет с небольшими затруднениями оценивать эффективность новых образцов программных средств защиты в компьютерных системах.</p> <p align="center">Отлично</p> <p>Умеет без затруднений оценивать эффективность новых образцов программных средств защиты в компьютерных системах.</p>

ПСК.6

Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПСК.6 Способность применять языки, системы и инструментальные средства</p>	<p>Знать языки, системы и инструментальные средства программирования. Уметь работать с программными средствами</p>	<p align="center">Неудовлетворител</p> <p>Не может применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного,</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности	прикладного, системного и специального назначения. Владеть навыками применения языков, систем и инструментальных средств программирования, работы с программными средствами прикладного, системного и специального назначения в профессиональной деятельности	<p>Неудовлетворител системного и специального назначения в организации работы и анализа сетевого сканера.</p> <p>Удовлетворительн Может применять работать с программными средствами прикладного, системного и специального назначения в организации работы. Не может анализировать результаты работы сетевого сканера.</p> <p>Хорошо Может применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в организации работы. Не может анализировать результаты работы сетевого сканера.</p> <p>Отлично Может применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в организации работы и анализа сетевого сканера.</p>

ПСК.2

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПСК.2 способность проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей	Знать потенциальные уязвимости программного кода. Уметь проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей. Владеть методами анализа программного кода с целью поиска потенциальных уязвимостей и	<p>Неудовлетворител Не умеет проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей.</p> <p>Удовлетворительн Умеет с большими затруднениями проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей.</p> <p>Хорошо Умеет с небольшими затруднениями</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
	недокументированных возможностей.	<p style="text-align: center;">Хорошо</p> проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей.
		<p style="text-align: center;">Отлично</p> Умеет без затруднений проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей.

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
------------------------------------	--	---

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ПК.1 Способность взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий</p> <p>ПСК.2 способность проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей</p> <p>ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности</p> <p>ПК.4 способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности</p> <p>ПСК.6 Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности</p>	<p>Предотвращение уязвимостей на этапе реализации</p> <p>Защищаемое контрольное мероприятие</p>	<p>Умеет предотвращать появление уязвимостей различного уровня на этапе разработки программ.</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ПСК.5 способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах</p> <p>ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований</p> <p>ПК.9 Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем</p> <p>ПК.11 способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи</p> <p>ПК.13 способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей</p> <p>ПК.23 Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами</p>	<p>Актуальные уязвимости современного программного обеспечения</p> <p>Защищаемое контрольное мероприятие</p>	<p>Умеет находить уязвимости в современном ПО.</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	Итоговое контрольное мероприятие Письменное контрольное мероприятие	Умеет решать задачи пройденного курса.

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 соответствии с требованиями к разработке безопасного ПО	30
Анализ и оценка программ соучеников на соответствие 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 технологий и в соответствии 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