МИНОБРНАУКИ РОССИИ

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

Институт компьютерных наук и технологий

Авторы-составители: **Кривилёва Анастасия Сергеевна**
Мустакимова Яна Романовна
Неверов Алексей Валерьевич

Рабочая программа дисциплины

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

Код УМК 68795

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

Пермь, 2022

1. Наименование дисциплины

Защита информационных систем от вредоносных программ

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 **Защита информационных систем от вредоносных программ** у обучающегося должны быть сформированы следующие компетенции:

10.05.01 Компьютерная безопасность (специализация : Разработка защищенного программного обеспечения)

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

ПК.5 Способен проводить регламентные работы с программными (программно-техническими) средствами защиты информации

Индикаторы

ПК.5.1 Анализирует необходимость проведения регламентных работ с программными (программно-техническими) средствами защиты информации

ПК.5.2 Применяет на практике знания по проведению регламентных работ с программными (программно-техническими) средствами защиты информации

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

Индикаторы

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 (специализация: Разработка защищенного программного обеспечения)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	13
Объем дисциплины (з.е.)	4
Объем дисциплины (ак.час.)	144
Контактная работа с преподавателем (ак.час.), в том числе:	56
Проведение лекционных занятий	28
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	88
Формы текущего контроля	Защищаемое контрольное мероприятие (2) Письменное контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (13 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Защита информационных систем от вредоносных программ.Первый семестр

Вредоносное программное обеспечение

Классификация вредоносного программного обеспечения

1. Понятие вредоносного ПО;
2. Компьютерные вирусы;
2.1. основные характеристики;
2.2. пути заражения;
2.3. проявления;
2.4. последствия;
3. Троянские программы;
3.1. основные характеристики;
3.2. пути заражения;
3.3. проявления;
3.4. последствия;
4. Черви;
4.1. основные характеристики;
4.2. пути заражения;
4.3. проявления;
4.4. последствия;
5. Эксплойты.
6. Другие виды вредоносного ПО.
7. Основные характеристики вредоносных программ:
7.1. Целевая среда;
7.2. Объекты-носители;
7.3. Механизмы запуска;
7.4. Механизмы распространения;
7.5. Механизмы защиты;
7.6. Вредоносное действие.

Компьютерные вирусы

1. Понятие компьютерного вируса;
2. Классификация компьютерных вирусов;
3. Эволюция компьютерных вирусов;
4. Основные приемы заражения программ вирусами;
5. Компьютерные вирусы в различных операционных системах (DOS, Windows, UNIX);
6. Примеры компьютерных вирусов.

Черви

1. Понятие компьютерного червя;
2. Основные отличия червя от вируса;
3. Анатомия компьютерного червя;
4. Принципы работы и заражения;
5. Пути распространения червей;
6. Примеры червей.

Троянские программы

1. Понятие троянской программы.

2. Роль троянской программы в распространении вредоносно ПО;
3. Примеры троянских программ.

Другие виды вредоносных программ

1. Exploits.
2. Rootkits
3. Вирусные бот-сети

Организация защиты от вредоносных программ

Методы обнаружения и уничтожения вредоносных программ

1. Сигнатурный поиск;
2. Эвристический анализ;
3. Методики моделирования виртуальных процессоров и ложный запуск программ;
4. Проактивная защита;

Классификация антивирусных программ

1. Понятие антивирусной программы;
2. Функции антивирусного программного обеспечения
3. Программы-сканеры;
4. Программы-мониторы;
5. Системы проактивной защиты;
6. Характеристики наиболее популярных систем антивирусной защиты

Организация многоуровневой системы защиты от вредоносных программ

1. Подходы к организации защиты от вредоносных программ;
2. Принципы организации многоуровневой системы защиты от вредоносных программ;
3. Защита клиентов и серверов;
4. Защита сервисов;
5. Защита периметра корпоративной сети;
6. Защита демилитаризованной зоны;
7. Повышение эффективности многоуровневой защиты (использование аппаратно-программных комплексов, использование многоядерных антивирусных систем и т.д.)

Итоговое контрольное мероприятие

Итоговая контрольная работа по всем пройденным темам курса

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. Гошко, С. В. Технологии борьбы с компьютерными вирусами : практическое пособие / С. В. Гошко. — Москва : СОЛОН-ПРЕСС, 2016. — 351 с. — ISBN 978-5-91359-059-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. http://www.iprbookshop.ru/90288

2. Касперский Евгений Компьютерные вирусы в MS-DOS/Евгений Касперский.-М.:"ЭДЭЛЬ"-"Ренессанс",1992, ISBN 5-85308-001-6.-176.

3. Крис, Касперски Фундаментальные основы хакерства. Искусство дизассемблирования / Касперски Крис. — Москва : СОЛОН-Р, 2016. — 446 с. — ISBN 5-93455-175-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. http://www.iprbookshop.ru/90401

Дополнительная:

1. Гошко С. В. Энциклопедия по защите от вирусов/С. В. Гошко.-М.:СОЛОН-Пресс,2004, ISBN 5-98003-129-4.-304.

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
Портал "Лаборатории Касперского" по вредоносному ПО https://securelist.com/

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

Образовательный процесс по дисциплине **Защита информационных систем от вредоносных программ** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине "Защита информационных систем от вредоносных программ" 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).

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
Защита информационных систем от вредоносных программ

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

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.1.2 Выполняет тестирование программного кода	Знать основные методы тестирования программного кода. Уметь применять методы тестирования программного кода. Владеть навыками тестирования программного кода при решении профессиональных задач.	**Неудовлетворител** Не знает основные методы тестирования программного кода. Не умеет применять методы тестирования программного кода. 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	Знать основные методы и средства анализа программного кода. Уметь применять основные	**Неудовлетворител** Не знает основные методы и средства анализа программного кода. Не умеет применять основные методы и

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
кода	методы и средства анализа программного кода. Владеть навыками применения методов и средств анализа программного кода при решении профессиональных задач.	**Неудовлетворител** 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** 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.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн 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. 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.5

Способен проводить регламентные работы с программными (программно-техническими) средствами защиты информации

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.5.1 Анализирует необходимость проведения регламентных работ с программными (программно-техническими) средствами защиты информации	Знать содержание регламентных работ с программными (программно-техническими) средствами защиты информации. Уметь доказывать необходимость проведения регламентных работ с программными (программно-техническими) средствами	**Неудовлетворител** Не знает содержание регламентных работ с программными (программно-техническими) средствами защиты информации. Не умеет доказывать необходимость проведения регламентных работ с программными (программно-техническими) средствами защиты информации. Не владеет методами анализа необходимости проведения регламентных работ с

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
	защиты информации. Владеть методами анализа необходимости проведения регламентных работ с программными (программно-техническими) средствами защиты информации.	**Неудовлетворител** программными (программно-техническими) средствами защиты информации. **Удовлетворительн** Знает содержание регламентных работ с программными (программно-техническими) средствами защиты информации. Не умеет доказывать необходимость проведения регламентных работ с программными (программно-техническими) средствами защиты информации. Не владеет методами анализа необходимости проведения регламентных работ с программными (программно-техническими) средствами защиты информации. **Хорошо** Знает содержание регламентных работ с программными (программно-техническими) средствами защиты информации. Умеет доказывать необходимость проведения регламентных работ с программными (программно-техническими) средствами защиты информации. Владеет не в полной мере методами анализа необходимости проведения регламентных работ с программными (программно-техническими) средствами защиты информации. **Отлично** Знает содержание регламентных работ с программными (программно-техническими) средствами защиты информации. Умеет доказывать необходимость проведения регламентных работ с программными (программно-техническими) средствами защиты информации. Владеет в полной мере методами анализа необходимости проведения регламентных работ с программными (программно-техническими) средствами защиты информации.
ПК.5.2 Применяет на практике знания по проведению регламентных работ с	Знать содержание регламентных работ с программными (программно-техническими) средствами	**Неудовлетворител** Не знает содержание регламентных работ с программными (программно-техническими) средствами защиты информации.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
программными (программно-техническими) средствами защиты информации	защиты информации. Уметь проводить регламентные работы с программными (программно-техническими) средствами защиты информации. Владеть навыками проведения регламентных работ с программными (программно-техническими) средствами защиты информации при решении профессиональных задач.	**Неудовлетворител** Не умеет проводить регламентные работы с программными (программно-техническими) средствами защиты информации. Не владеет навыками проведения регламентных работ с программными (программно-техническими) средствами защиты информации при решении профессиональных задач. **Удовлетворительн** Знает содержание регламентных работ с программными (программно-техническими) средствами защиты информации. Частично умеет проводить регламентные работы с программными (программно-техническими) средствами защиты информации. Не владеет навыками проведения регламентных работ с программными (программно-техническими) средствами защиты информации при решении профессиональных задач. **Хорошо** Знает содержание регламентных работ с программными (программно-техническими) средствами защиты информации. Умеет проводить регламентные работы с программными (программно-техническими) средствами защиты информации. Владеет не в полной мере навыками проведения регламентных работ с программными (программно-техническими) средствами защиты информации при решении профессиональных задач. **Отлично** Знает содержание регламентных работ с программными (программно-техническими) средствами защиты информации. Умеет проводить регламентные работы с программными (программно-техническими) средствами защиты информации. Владеет в полной мере навыками проведения регламентных работ с программными (программно-техническими) средствами защиты информации при решении

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично профессиональных задач.

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 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.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
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 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.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
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. 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 : Очная 2019

Вид мероприятия промежуточной аттестации : Экзамен
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 46 до 60
«неудовлетворительно» / «незачтено» менее 46 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.5.2 Применяет на практике знания по проведению регламентных работ с программными (программно-техническими) средствами защиты информации **ПК.5.1** Анализирует необходимость проведения регламентных работ с программными (программно-техническими) средствами защиты информации	Компьютерные вирусы **Письменное контрольное мероприятие**	Вид: письменный коллоквиумЗадача: дать письменный ответ на один из поставленных вопросов

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПСК.1.2 Выполняет тестирование программного кода **ОПСК.1.4** Осуществляет поиск потенциальных уязвимостей и недокументированных возможностей программного кода **ПК.1.3** Применяет методы и средства мониторинга и анализа защищенности компьютерных систем и сетей **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 **ОПСК.1.3** Применяет на практике методы и средства анализа программного кода	Методы обнаружения и уничтожения вредоносных программ **Защищаемое контрольное мероприятие**	Вид: лабораторная работыЦель: написать программу, реализующую сигнатурный поиск определенного компьютерного вирусаЗадачи:1. Провести анализ отдельного лабораторно образца вредоносной программы2. Выделить сигнатуру 3. Написать программу поиска найденной сигнатуры в массиве файлов. Тестовый набор должен содержать как зараженные, так и не зараженные файлы

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.1.3 Применяет методы и средства мониторинга и анализа защищенности компьютерных систем и сетей **ОПСК.1.4** Осуществляет поиск потенциальных уязвимостей и недокументированных возможностей программного кода **ОПСК.1.3** Применяет на практике методы и средства анализа программного кода **ОПСК.1.2** Выполняет тестирование программного кода **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.5.2** Применяет на практике знания по проведению регламентных работ с программными (программно-техническими) средствами защиты информации **ПК.5.1** Анализирует необходимость проведения регламентных работ с программными (программно-техническими) средствами защиты информации	Итоговое контрольное мероприятие **Защищаемое контрольное мероприятие**	Вид: лабораторная работаЦель: написать программу, реализующую модель эвристического анализатораЗадачи:1) Выделить набор эвристик для обнаружения вредоносных программ2) Сформировать модель эвристического анализатора на основе нечетких продукций3) Выполнить программную реализацию

Спецификация мероприятий текущего контроля

Компьютерные вирусы

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **14**

Показатели оценивания	Баллы
Ответ на 2й вопрос	10
Ответ на 1й вопрос	10

Методы обнаружения и уничтожения вредоносных программ

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **14**

Показатели оценивания	Баллы
Написанная программа не попускает более 1% ложных срабатываний на незараженных файлах их тестового набора	15
Написанная программа гарантировано обнаруживает файлы, содержащие сигнатуру вируса	15

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **18**

Показатели оценивания	Баллы
Эвристический анализатор должен осуществлять поиск потенциально зараженных в тестовом наборе файлов с точностью не менее 80%	10
Эвристический анализатор может определять некоторые конкретные вирусы, используя сигнатурный анализ как часть эвристик	10
Эвристический анализатор должен определять тип заражения	10
Эвристический анализатор должен делать заключения «заражен – не заражен» для каждого из файлов тестового массива	10