

МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности и систем связи

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

Рабочая программа дисциплины

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ ОТ ВРЕДНОСНЫХ ПРОГРАММ

Код УМК 68795

Утверждено
Протокол №6
от «26» июня 2020 г.

Пермь, 2020

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

ПК.19 Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем

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

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

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	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 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. 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 // Электронно-библиотечная система IPR BOOKS : [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 // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/90401.html>

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-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).

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**

ПК.3

Способность к анализу и формализации поставленных задач в области информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности	Знать методы анализа и формализации поставленных задач в области информационной безопасности Владеть методами анализа и формализации поставленных задач в области информационной безопасности	Неудовлетворител Не способен к анализу и формализации поставленных задач в области информационной безопасности Удовлетворительн Знает основные методы анализа и формализации поставленных задач в области информационной безопасности Хорошо Знает основные методы анализа и формализации поставленных задач в области информационной безопасности и умеет применять их на практике Отлично Знает различные методы анализа и формализации поставленных задач в области информационной безопасности, умеет применять их на практике, оценивать их эффективность

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 потенциальные уязвимости компьютерных систем. Уметь проводить экспериментальные исследования компьютерных систем с целью выявления уязвимостей. Владеть методами проведения экспериментального исследования компьютерных систем.	Неудовлетворител Не умеет проводить экспериментальные исследования компьютерных систем с целью выявления уязвимостей Удовлетворительн Знает основные методы и приемы проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей Хорошо Знает основные методы и приемы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
	систем с целью выявления уязвимостей.	<p align="center">Хорошо</p> проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей, умеет применять их на практике <p align="center">Отлично</p> Знает различные методы и приемы проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей, умеет самостоятельно применять их на практике, анализировать их эффективность

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
<p>ПК.23 Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами</p>	Знать приемы организации защиты информации техническими и программными средствами. Уметь организовать защиту информации техническими и программными средствами. Владеть приемами антивирусной защиты при работе с компьютерными системами	<p align="center">Неудовлетворител</p> Не умеет организовывать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами <p align="center">Удовлетворительн</p> Знает базовые приемы организации защиты информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами <p align="center">Хорошо</p> Знает базовые приемы организации защиты информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами, умеет применять их на практике <p align="center">Отлично</p> Знает различные методы и приемы организации защиты информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами, умеет самостоятельно применять их на практике, анализировать их эффективность

ПК.19

Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.19 Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем	Знать составляющие системы обеспечения информационной безопасности компьютерных систем Уметь принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем	Неудовлетворител Не может принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем Удовлетворительн Может выполнять элементарные операции при эксплуатации системы обеспечения информационной безопасности компьютерных систем Хорошо Может работать с системами обеспечения информационной безопасности компьютерных систем с использованием инструкций, под контролем более опытных коллег Отлично Может самостоятельно эксплуатировать системы обеспечения информационной безопасности компьютерных систем

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
ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований	Знать основы информационной безопасности компьютерных систем. Уметь провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований Владеть методами выбора рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований	Неудовлетворител Не может провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований Удовлетворительн Может со значительными затруднениями провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований Хорошо Может выбрать оптимальное решение по уровню обеспечения информационной

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Хорошо</p> безопасности компьютерных систем из широкого набора средств <p style="text-align: center;">Отлично</p> Может выбрать оптимальное решение оптимальное решение по уровню обеспечения информационной безопасности компьютерных систем из широкого набора средств и обосновать его

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>	Знать составляющие системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, формальные модели политик безопасности, политик управления доступом и информационными потоками 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 style="text-align: center;">Неудовлетворител</p> Не может 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 style="text-align: center;">Удовлетворительн</p> Знает основные требования к разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы <p style="text-align: center;">Хорошо</p> Знает основные требования к разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, умеет разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах <p style="text-align: center;">Отлично</p> Знает различные, в т.ч. международные, требования к разработке системы защиты информации предприятия и подсистемы информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Отлично</p> <p>компьютерной системы, умеет разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками 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 программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности</p>	<p>Знать языки, системы и инструментальные средства программирования. Уметь работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности</p>	<p style="text-align: center;">Неудовлетворител</p> <p>Не умеет применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности</p> <p style="text-align: center;">Удовлетворительн</p> <p>Умеет применять стандартные средства программирования</p> <p style="text-align: center;">Хорошо</p> <p>Умеет применять различные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности</p> <p style="text-align: center;">Отлично</p> <p>Умеет применять стандартные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности, оценивать их эффективность в заданных условиях</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
<p>ПСК.2 способность проводить</p>	<p>Знать потенциальные уязвимости программного кода.</p>	<p style="text-align: center;">Неудовлетворител</p> <p>Не может проводить анализ программного</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей</p>	<p>Уметь проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей. Владеть методами анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей.</p>	<p>Неудовлетворител кода с целью поиска потенциальных уязвимостей и недокументированных возможностей</p> <p>Удовлетворительн Владеет базовыми навыками анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей</p> <p>Хорошо Может проводить анализ программного кода с с целью поиска потенциальных уязвимостей и недокументированных возможностей с использованием различных средств</p> <p>Отлично Может проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей с использованием различных средств, обобщать и анализировать данные</p>

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
ПСК.2 способность проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей ПСК.6 Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований	Компьютерные вирусы Письменное контрольное мероприятие	Вид: письменный коллоквиум Задача: дать письменный ответ на один из поставленных вопросов

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<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>ПСК.6 Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности</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.13 способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей</p>	<p>Методы обнаружения и уничтожения вредоносных программ</p> <p>Защищаемое контрольное мероприятие</p>	<p>Вид: лабораторная работы Цель: написать программу, реализующую сигнатурный поиск определенного компьютерного вируса Задачи: 1. Провести анализ отдельного лабораторно образца вредоносной программы 2. Выделить сигнатуру 3. Написать программу поиска найденной сигнатуры в массиве файлов. Тестовый набор должен содержать как зараженные, так и не зараженные файлы</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<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>ПСК.6 Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности</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.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>ПК.13 способность к проведению экспериментального исследования компьютерных</p>	<p>Итоговое контрольное мероприятие</p> <p>Защищаемое контрольное мероприятие</p>	<p>Вид: лабораторная работа Цель: написать программу, реализующую модель эвристического анализатора Задачи:1) Выделить набор эвристик для обнаружения вредоносных программ2) Сформировать модель эвристического анализатора на основе нечетких продукций3) Выполнить программную реализацию</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>систем с целью выявления уязвимостей</p> <p>ПК.19 Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем</p> <p>ПК.23 Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами</p>		

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