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
Айдаров Юрий Рафаэлевич
Неверов Алексей Валерьевич

Рабочая программа дисциплины

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

Код УМК 81387

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 вариативную 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.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.14 способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения

ПК.15 Способность оценивать эффективность системы защиты информации в компьютерных системах

ПК.18 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы

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.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций

ПК.6 Способность разрабатывать математические модели защищаемых систем и 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

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.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.)	5
Объем дисциплины (ак.час.)	180
Контактная работа с преподавателем (ак.час.), в том числе:	70
Проведение лекционных занятий	28
Проведение практических занятий, семинаров	0
Проведение лабораторных работ, занятий по иностранному языку	42
Самостоятельная работа (ак.час.)	110
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (3)
Формы промежуточной аттестации	Экзамен (13 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Защита информационных систем от вредоносных программ. Первый семестр
Защита ИС от ВНП

Понятие и классификация ВНП
Тема 1. 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.

Тема 2. 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.

Тема 3. 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.

Тема 4. Троянские программы.
1. Понятие троянской программы.
2. Роль троянской программы в распространении вредоносно ПО;
3. Примеры троянских программ.

Тема 5. Exploits
1. Exploits.
2. Rootkits
3. Вирусные бот-сети

Особенности и способы внедрения ВНП

Классификация способов внедрения вредоносного ПО

Понятие и классификация способов противодействия ВНП

Тема 6. 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

Тема 7. 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.)

Разработка антивирусного программного обеспечения

Тема 8. Методы обнаружения и уничтожения вредоносных программ
1. Сигнатурный поиск;
2. Эвристический анализ;
3. Методики моделирования виртуальных процессоров и ложный запуск программ;
4. Проактивная защита;

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 // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/90288

2. Соловьев Л. Н. Вредоносные программы : расследование и предупреждение преступлений/Л. Н. Соловьев.-М.:Собрание,2004, ISBN 5-9606-0003-X.-224.-Библиогр.: с. 215-222

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

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

Дополнительная:

1. Антивирусная защита компьютерных систем:учебный курс : Курс создан при финансовой поддержке компании "Лаборатория Касперского"

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

3. 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

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://securelist.com/ Лаборатория Касперского

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 и критерии их оценивания

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.13 способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей	Знать основные уязвимости компьютерных систем. Уметь проводить экспериментальные исследования компьютерных систем. Владеть навыками проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей	**Неудовлетворител** Не умеет проводить экспериментальные исследования компьютерных систем с целью выявления уязвимостей **Удовлетворительн** Знает базовые принципы проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей **Хорошо** Знает базовые принципы проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей и умеет применять их на практике **Отлично** Умеет проводить экспериментальные исследования компьютерных систем с целью выявления уязвимостей с помощью различных средств и методов
ПК.14 способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения	Знать базовые модели решения профессиональной задачи. Уметь обосновывать правильность выбранной модели решения профессиональной задачи, Владеть навыками обработки результатов экспериментов	**Неудовлетворител** Не может обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения **Удовлетворительн** Умеет работать с базовыми моделями решения профессиональной задачи **Хорошо** Умеет работать с базовыми моделями решения профессиональной задачи, анализировать полученные результаты **Отлично** Умеет работать с различными моделями решения профессиональной задачи, самостоятельно выбирать их для решения

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично задачи и анализировать полученные результаты
ПК.23 Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	Знать технические и программные средства защиты данных. Уметь организовать защиту информации техническими и программными средствами. Владеть приемами антивирусной защиты при работе с компьютерными системами	**Неудовлетворител** Не может организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами **Удовлетворительн** Умеет работать с базовыми средствами организации защиты информации техническими и программными средствами **Хорошо** Умеет работать с различными средствами организации защиты информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами **Отлично** Умеет работать с различными средствами организации защиты информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами, анализировать их эффективность, самостоятельно выбирать оптимальное в указанных условиях
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 недокументированных возможностей.	**Неудовлетворител** Не может проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей **Удовлетворительн** Владеет базовыми навыками анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей **Хорошо** Может проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей с использованием различных средств **Отлично** Может проводить анализ программного кода с целью поиска потенциальных уязвимостей

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично и недокументированных возможностей с использованием различных средств, обобщать и анализировать полученные данные
ПК.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций	Знать существующие источники информации для аналитических обзоров по вопросам обеспечения информационной безопасности компьютерных систем Уметь осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций Владеть навыками обработки полученной информации.	**Неудовлетворител** Не способен осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций **Удовлетворительн** Умеет на базовом уровне осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем **Хорошо** Умеет использовать различные источники информации для аналитических обзоров по вопросам обеспечения информационной безопасности компьютерных систем и обобщать полученную информацию **Отлично** Умеет осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций
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.	**Неудовлетворител** Не может проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем **Удовлетворительн** Владеет базовыми методами анализа проектных решений по обеспечению информационной безопасности компьютерных систем **Хорошо** Владеет различными методами анализа проектных решений по обеспечению информационной безопасности компьютерных систем **Отлично**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Владеет различными методами анализа проектных решений по обеспечению информационной безопасности компьютерных систем, может анализировать полученные результаты
ПК.11 способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи	Знать механизмы обеспечения безопасности. Уметь оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи. Владеть методами оценки степени надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи.	**Неудовлетворител** Не способен оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи **Удовлетворительн** Знает базовые методы оценки степени надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи **Хорошо** Знает базовые методы оценки степени надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи и умеет применять их на практике **Отлично** Знает различные сложные методы оценки степени надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи и умеет применять их на практике
ПК.6 Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем	Знать составляющие системы обеспечения информационной безопасности компьютерных систем. Уметь разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем Владеть математическим аппаратом для разработки математических моделей защищаемых систем и системы обеспечения информационной безопасности компьютерных систем	**Неудовлетворител** Не может разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем **Удовлетворительн** Знает базовые модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем **Хорошо** Знает базовые модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем, умеет применять их на практике **Отлично** Умеет строить и анализировать сложные модели защищаемых систем и системы

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично обеспечения информационной безопасности компьютерных систем, применять их на практике
ПК.15 Способность оценивать эффективность системы защиты информации в компьютерных системах	Знать составляющие системы защиты информации в компьютерных системах. Уметь оценивать эффективность системы защиты информации в компьютерных системах. Владеть методами оценки эффективности системы защиты информации в компьютерных системах.	**Неудовлетворител** Не умеет оценивать эффективность системы защиты информации в компьютерных системах **Удовлетворительн** Владеет базовыми приемами оценки эффективность системы защиты информации в компьютерных системах **Хорошо** Владеет различными приемами оценки эффективность системы защиты информации в компьютерных системах **Отлично** Владеет различными приемами оценки эффективность системы защиты информации в компьютерных системах, может выбрать оптимальный
ПК.18 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Знать составляющие системы управления информационной безопасностью компьютерной системы. Уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы. Владеть кавыками анализа системы управления информационной безопасностью компьютерной системы.	**Неудовлетворител** Не умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы **Удовлетворительн** Может сформулировать основные предложения по совершенствованию системы управления информационной безопасностью компьютерной системы **Хорошо** Может сформулировать четкие и понятные предложения по совершенствованию системы управления информационной безопасностью компьютерной системы **Отлично** Может сформулировать четкие и понятные предложения по совершенствованию системы управления информационной безопасностью компьютерной системы, обосновать их
ПСК.6 Способность применять языки, системы и	Знать языки, системы и инструментальные средства программирования.	**Неудовлетворител** Не умеет применять языки, системы и инструментальные средства

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности	Уметь работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности	**Неудовлетворител** программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности **Удовлетворительн** Умеет использовать основные языки, системы и инструментальные средства программирования **Хорошо** Умеет использовать различные языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности **Отлично** Умеет использовать различные языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности, выбирает наилучшие в указанных условиях
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	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	**Неудовлетворител** 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 **Удовлетворительн** Знает основные требования к разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы **Хорошо** 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

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо информационными потоками в компьютерных системах **Отлично** Знает различные, в т.ч. международные, 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
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 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	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	**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**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
	заданных требований.	**Хорошо** Может выбрать из широкого набора средств рационально решение по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований **Отлично** Может выбрать оптимальное решение по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований из широкого набора средств и обосновать его

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

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 79 до 60
«неудовлетворительно» / «незачтено» менее 79 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Понятие и классификация ВНП **Входное тестирование**	Письменная работа на знание классификации ВНП
ПК.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций **ПСК.6** Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности **ПК.18** способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Особенности и способы внедрения ВНП **Защищаемое контрольное мероприятие**	Вид: письменный коллоквиумЗадача: дать письменный ответ на один из поставленных вопросов

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПСК.2 способность проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей **ПК.13** способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей **ПК.15** Способность оценивать эффективность системы защиты информации в компьютерных системах **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	Понятие и классификация способов противодействия ВНП **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	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.6 Способность разрабатывать математические модели защищаемых систем и 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 **ПК.9** Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем **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.14** способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и	Разработка антивирусного программного обеспечения **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

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
теоретические решения		

Спецификация мероприятий текущего контроля

Понятие и классификация ВНП

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**
Проходной балл: **0**

Показатели оценивания	Баллы

Особенности и способы внедрения ВНП

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **19.5**

Показатели оценивания	Баллы
Ответ на 2й вопрос	15
Ответ на 1й вопрос	15

Понятие и классификация способов противодействия ВНП

Продолжительность проведения мероприятия промежуточной аттестации: **14 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **19.5**

Показатели оценивания	Баллы
Разработан базовый алгоритм сигнатурного поиска	10
Сигнатурный поиск отрабатывает на тестовом наборе файлов	10
Сигнатурный поиск не дает ложных срабатываний (сигнатура выбрана корректно)	10

Разработка антивирусного программного обеспечения

Продолжительность проведения мероприятия промежуточной аттестации: **16 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **40**

Показатели оценивания	Баллы
Разработан базовый эвристический анализатор	10
Точность и чувствительность анализатора составляют более 90% на тестовом наборе файлов	10
Точность и чувствительность анализатора составляют более 75% на валидационном наборе	10

файлов	
Точность и чувствительность анализатора составляют более 50% на любом наборе файлов	10