

**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 « Б.1 » образовательной программы по направлениям подготовки (специальностям):

Направление: **09.03.02** Информационные системы и технологии  
направленность Безопасность информационных систем

### **3. Планируемые результаты обучения по дисциплине**

В результате освоения дисциплины **Защита информационных систем от вредоносных программ** у обучающегося должны быть сформированы следующие компетенции:

**09.03.02** Информационные системы и технологии (направленность : Безопасность информационных систем)

**ПК.17** способность оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях

**ПК.21** способность обеспечивать безопасность и целостность данных информационных систем и технологий

**ПК.4** способность проводить выбор исходных данных для проектирования

**ПК.8** способность к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию

#### 4. Объем и содержание дисциплины

<b>Направления подготовки</b>	09.03.02 Информационные системы и технологии (направленность: Безопасность информационных систем)
<b>форма обучения</b>	очная
<b>№№ триместров, выделенных для изучения дисциплины</b>	6
<b>Объем дисциплины (з.е.)</b>	5
<b>Объем дисциплины (ак.час.)</b>	180
<b>Контактная работа с преподавателем (ак.час.), в том числе:</b>	70
<b>Проведение лекционных занятий</b>	28
<b>Проведение практических занятий, семинаров</b>	0
<b>Проведение лабораторных работ, занятий по иностранному языку</b>	42
<b>Самостоятельная работа (ак.час.)</b>	110
<b>Формы текущего контроля</b>	Входное тестирование (1) Защищаемое контрольное мероприятие (3)
<b>Формы промежуточной аттестации</b>	Экзамен (6 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 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. Соловьев Л. Н. Вредоносные программы : расследование и предупреждение преступлений/Л. Н. Соловьев.-М.:Собрание,2004, ISBN 5-9606-0003-Х.-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-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](http://student.psu.ru)).

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ ([student.psu.ru](http://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
<p><b>ПК.8</b> способность к установке, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию</p>	<p>Знать этапы работ с техническими средствами. Уметь выполнять установку, отладку программных и настройку технических средств для ввода информационных систем в опытную и промышленную эксплуатацию</p>	<p align="center"><b>Неудовлетворител</b> Не умеет работать с техническими средствами для ввода информационных систем в опытную и промышленную эксплуатацию.</p> <p align="center"><b>Удовлетворительн</b> Работает с наиболее известными техническими средствами для ввода информационных систем в опытную и промышленную эксплуатацию.</p> <p align="center"><b>Хорошо</b> Работает с различными техническими средствами для ввода информационных систем в опытную и промышленную эксплуатацию.</p> <p align="center"><b>Отлично</b> Способен самостоятельно анализировать и выбирать оптимальные технические средства для ввода информационных систем в опытную и промышленную эксплуатацию.</p>
<p><b>ПК.21</b> способность обеспечивать безопасность и целостность данных информационных систем и технологий</p>	<p>Знать базовые принципы обеспечения безопасности и целостности данных информационных систем и технологий. Уметь обеспечивать безопасность и целостность данных информационных систем и технологий</p>	<p align="center"><b>Неудовлетворител</b> Не может обеспечивать безопасность и целостность данных информационных систем и технологий</p> <p align="center"><b>Удовлетворительн</b> Знает базовые принципы обеспечения безопасности и целостности данных информационных систем и технологий.</p> <p align="center"><b>Хорошо</b> Знает базовые принципы обеспечения безопасности и целостности данных информационных систем и технологий и умеет применять их на практике.</p> <p align="center"><b>Отлично</b> Знает и умеет различные методы и средства обеспечения безопасности и целостности данных информационных систем и</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ПК.17</b> способность оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях</p>	<p>Знать способы представления рабочих результатов. Уметь оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях. Владеть навыками оформления полученных рабочих результатов в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях.</p>	<p><b>Отлично</b> технологий и умеет применять их на практике.</p> <p><b>Неудовлетворител</b> Не способен оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях</p> <p><b>Удовлетворительн</b> Способен на базовом уровне оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях</p> <p><b>Хорошо</b> Способен с помощью инструкций оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях</p> <p><b>Отлично</b> Способен полностью самостоятельно оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях</p>
<p><b>ПК.4</b> способность проводить выбор исходных данных для проектирования</p>	<p>Знать понятие проектирования. Уметь проводить выбор исходных данных для проектирования</p>	<p><b>Неудовлетворител</b> Не может проводить выбор исходных данных для проектирования.</p> <p><b>Удовлетворительн</b> Владеет базовыми методами выбора исходных данных для проектирования.</p> <p><b>Хорошо</b> Владеет базовыми методами выбора исходных данных для проектирования, умеет применять их на практике.</p> <p><b>Отлично</b> Владеет различными сложными методами выбора исходных данных для проектирования, умеет применять их на практике.</p>

## 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
<b>Входной контроль</b>	Понятие и классификация ВНП <b>Входное тестирование</b>	Письменная работа на знание классификации ВНП
<b>ПК.17</b> способность оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях	Особенности и способы внедрения ВНП <b>Защищаемое контрольное мероприятие</b>	Вид: письменный коллоквиум Задача: дать письменный ответ на один из поставленных вопросов
<b>ПК.4</b> способность проводить выбор исходных данных для проектирования	Понятие и классификация способов противодействия ВНП <b>Защищаемое контрольное мероприятие</b>	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

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p><b>ПК.8</b> способность к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию</p> <p><b>ПК.21</b> способность обеспечивать безопасность и целостность данных информационных систем и технологий</p>	<p>Разработка антивирусного программного обеспечения</p> <p><b>Защищаемое контрольное мероприятие</b></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>

### Спецификация мероприятий текущего контроля

#### Понятие и классификация ВМП

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 ВМП

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 ВМП

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**

<b>Показатели оценивания</b>	<b>Баллы</b>
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 файлов	10
Точность и чувствительность анализатора составляют более 50% на любом наборе файлов	10