

**Программа учебной дисциплины: Анализ программных реализаций алгоритмов защиты**

Утверждена  
Кафедрой компьютерной  
безопасности МИЭМ НИУ ВШЭ  
Протокол № 5 от «24» июня 2019 г.

Академическим советом ОП 25.06.2019 г

|                               |  |
|-------------------------------|--|
| Автор                         | Сорокин А.В. ( <a href="mailto:asorokin@hse.ru">asorokin@hse.ru</a> );<br>Золотов П.А. ( <a href="mailto:pzolotov@hse.ru">pzolotov@hse.ru</a> ). |
| Число кредитов                | 3  |
| Контактная работа (час.)      | 32   |
| Самостоятельная работа (час.) | 120  |
| Курс                          | 5 курс   |
| Формат изучения дисциплины    | Без использования онлайн курса   |

**I. ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ**

Целью освоения дисциплины дисциплину «Анализ программных реализаций алгоритмов защиты» является формирование у студентов навыков, необходимых для решения предусмотренных ФГОС специальности 10.05.01 "Компьютерная безопасность" следующих профессиональных задач:

- Разработка математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов;
- Подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований;
- Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации;
- Применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;
- Выполнение экспериментально-исследовательских работ при проведении сертификации программно-аппаратных средств защиты и анализ результатов.

В результате изучения дисциплины студент должен:

**Знать:**

- методы анализа программного обеспечения;
- основные уязвимости систем защиты информации;
- основные средства и методы анализа программных реализаций;
- защитные механизмы и средства обеспечения безопасности информационных

систем;

- методы оценки уровня защищенности компьютерных систем;

**Уметь:**

- анализировать программное обеспечение средств защиты компьютерных систем;
- исследовать системы защиты компьютерных систем и их составляющих с целью обнаружения уязвимостей;
- анализировать компьютерные системы и их составляющие с целью определения уровня защищенности и доверия;

**Владеть:**

- методами анализа программного обеспечения;
- основными методами верификации программ;
- методами исследования средств защиты компьютерных систем с точки зрения анализа их программных реализаций.

Дисциплина «Анализ программных реализаций алгоритмов защиты» относится к числу дисциплин вариативной части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин в соответствии с образовательным стандартом по специальности 10.05.01 «Компьютерная безопасность»:

- Информатика – знание основных понятий информатики;
- Языки программирования – знание языков программирования высокого уровня и языка ассемблера персонального компьютера, владение навыками разработки, документирования, тестирования и отладки программ;
- Основы информационной безопасности – знание основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации, владение профессиональной терминологией в области информационной безопасности;
- Операционные системы – знание принципов построения современных операционных систем и особенностей их применения, владение навыками конфигурирования и администрирования операционных систем;
- Защита в операционных системах – знание защитных механизмов и средств обеспечения безопасности операционных систем, умение формулировать и настраивать политику безопасности основных операционных систем;
- Защита программ и данных – знание основных средств и методов анализа программных реализаций, владение навыками анализа программных реализаций;
- Компьютерные сети – знание эталонной модели взаимодействия открытых систем, типовых структур и принципов организации компьютерных сетей, основ интернет-технологий, владение навыками конфигурирования локальных компьютерных сетей и реализации сетевых протоколов с помощью программных средств;

- Криптографические методы защиты информации – знание основных видов симметричных и асимметричных криптографических алгоритмов, средств и методов хранения аутентификационной информации, владение криптографической терминологией.

Дисциплина Анализ программных реализаций алгоритмов защиты является предшествующей для изучения следующих базовых дисциплин: Криптографические протоколы, Основы построения защищенных баз данных, а также дисциплин вариативной части профессионального цикла, предусмотренных примерным учебным планом. Знания и практические навыки, полученные из дисциплины Анализ программных реализаций алгоритмов защиты.

## II. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

*Тема 1. Задачи анализа программных реализаций алгоритмов защиты информации.*

Актуальность задачи анализа программных реализаций. Методология и основные этапы работ по анализу. Необходимые сведения о вычислительной системе, языках программирования, операционных системах, локальных и глобальных вычислительных сетях.

*Тема 2. Методы восстановления алгоритмов защиты информации по их программным реализациям. (Лекции – 10 часов, практика – 18 часов)*

Основные подходы к восстановлению алгоритмов защиты. Метод экспериментов с черным ящиком. Статический метод. Динамический метод. Вопросы автоматизации анализа.

*Тема 3. Оценка надежности встроенной криптографической защиты типовых программных продуктов (Лекции – 2 часа)*

Системы защиты, использующие криптографически слабые шифры. Системы с ключевой информацией в зашифрованном файле. Системы с эквивалентными ключами. Регуляторы стойкости.

*Тема 4. Анализ программных методов генерации ключей (Лекции – 2 часа).*

Типовые программные методы генерации ключевой информации. Теоретические методы анализа программ генерации ключей. Экспериментальные методы оценки криптографических качеств ключей. Анализ способов распределения ключевой информации в вычислительной сети.

*Тема 5. Оценка надежности защиты с учетом работы в многопользовательской вычислительной сети (Лекции – 2 часа).*

Понятие криптографической закладки. Криптографические закладки в программах запускаемых командной строкой DOS. Типовые изъяны операционных систем. Атаки через сеть. Экспресс-анализ защищенности вычислительной системы при ее работе в локальных и глобальных вычислительных сетях.

### **III. ОЦЕНИВАНИЕ**

На текущем и промежуточном контроле знаний, в объеме изученного материала, студент должен продемонстрировать знание основ исследования программных реализаций алгоритмов защиты, методов анализа программных продуктов, принципы работы с анализаторами программ.

При выполнении домашних заданий и контрольной работы студент должен продемонстрировать:

- умение работать с программными средствами прикладного, системного и специального назначения;
- умение использовать языки и системы программирования, инструментальные средства для решения задач анализа программных продуктов;
- умение применять современные методы и средства исследований программных реализаций различных алгоритмов.

На итоговом контроле знаний студент должен продемонстрировать знания:

- основных уязвимостей систем защиты информации;
- основных методов анализа программного обеспечения;
- методов защиты программного обеспечения от изучения;
- защитных механизмов и средств обеспечения безопасности информационных систем;
- методов оценки уровня защищенности компьютерных систем.

Формы контроля:

Оценка знаний студентов на этапах промежуточной аттестации осуществляется во 2 модуле в форме коллоквиума, в 3 модуле – в форме приемки отчетов о выполнении домашних заданий - лабораторных работ. В ходе отчета о выполнении лабораторных работ студенту могут быть заданы вопросы по сути выполненной работы, о применяемых методах и средствах, а также вопросы теоретического характера по материалам курса.

### **IV. ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ**

Примеры оценочных материалов размещены на сайте дисциплины в системе LMS.

### **V. РЕСУРСЫ**

#### **1. Основная литература**

- Проскурин В.Г. Защита программ и данных. Учебное пособие для вузов – М.: Издательский центр «Академия», 2011 . – 200 с.
- Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб.

пособие для студ. высш. учеб. заведений. – М.: Издательский центр «Академия», 2006. – 256 с

## 2. Дополнительная литература

- О. Зайцев. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors. Обнаружение и защита. – СПб: «БХВ-Петербург». 2006. – 304 с.
- К. Касперски. Фундаментальные основы хакерства. – М: «СОЛОН-Р». 2005. – 448 с.
- К. Касперски. Техника защиты компакт-дисков от копирования. – СПб: «БХВ-Петербург». 2004. – 458 с.
- Дж. Козиол, Д. Личфилд, Д. Эйтел, К Энли, С. Эрен, Н. Мехта, Р. Хассель. Искусство взлома и защиты систем. – СПб: «Питер». 2006. – 416 с.
- Х. Майкл, Д. Лебланк. Защищенный код. – М.: «Русская редакция», 2004. – 704 с.
- Проблемы информационной безопасности. Компьютерные системы. – СПб: Издательство Политехнического университета

## 3. Программное обеспечение

| № п/п | Наименование                       | Условия доступа           |
|-------|------------------------------------|---------------------------|
| 1.    | Microsoft Visual Studio            | По договору               |
| 2.    | Microsoft Debugging Tools          | По договору               |
| 3.    | VMWare Workstation или Virtual Box | Свободное распространение |
| 4.    | Ucrypt                             | Свободное распространение |
| 5.    | Wreg                               | Свободное распространение |
| 6.    | Ida                                | Свободное распространение |
| 7.    | Turbo Debugger                     | Свободное распространение |
| 8.    | SoftIce                            | Свободное распространение |

## 4. Профессиональные базы данных, информационные справочные системы, интернет-ресурсы (электронные образовательные ресурсы)

| № п/п | Наименование                          | Условия доступа  |
|-------|---------------------------------------|--|
| 2.    | Электронно-библиотечная система Юрайт | URL: <a href="https://biblio-online.ru/">https://biblio-online.ru/</a> |

## 5. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе:

- ПЭВМ с доступом в Интернет (операционная система, офисные программы,

антивирусные программы);

– мультимедийный проектор с дистанционным управлением.

Учебные аудитории для лабораторных и самостоятельных занятий по дисциплине оснащены компьютерами с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде НИУ ВШЭ.