От автора

При подготовке учебного пособия «Антивирусная безопасность цифровой информации» автор использовал информацию из открытых источников. Цитирование осуществлялось исключительно в учебных целях и в объеме, оправданном целью цитирования, с указанием соответствующих источников заимствования, представленных в списке литературы данного пособия.

Использование информации, размещенной в учебном пособии, является использованием в понимании п. 1 ст. 1274 Гражданского кодекса Российской Федерации.

Автор выражает искреннюю признательность коллегам за профессиональную помощь и содействие при работе над учебным пособием «Антивирусная безопасность цифровой информации», а именно:

- генеральному директору ЗАО «ОКБ САПР», д-ру техн. наук, профессору Конявскому Валерию Аркадьевичу (официальный сайт https://okbsapr.ru);
- заместителю генерального директора ЗАО «ОКБ САПР», канд. филол. наук, доценту Конявской Светлане Валерьевне (официальный сайт https://okbsapr.ru);
- АО «Лаборатория Касперского» (официальный сайт https://kaspersky.ru);
- ИТ-энциклопедии «Вирусная энциклопедия Касперского», размещенной на официальном сайте АО «Лаборатория Касперского» (https://encyclopedia.kaspersky.ru);
- издательству «Познание» Казанского инновационного университета имени В.Г. Тимирясова (https://ieml.ru/podrazdeleniya-universiteta/izdatelstvo-poznanie);
- кафедре «Информационные технологии и безопасность» Казанского инновационного университета имени В.Г. Тимирясова (официальный сайт https://ieml.ru).
- кафедре «Системы информационной безопасности» Казанского национального исследовательского технического университета имени А.Н. Туполева — КАИ (официальный сайт https://kai.ru).

«... Мне кажется, компьютерные вирусы стоит рассматривать как форму жизни. Это многое говорит о природе человека: единственная форма жизни, которую мы создали к настоящему моменту, несет только разрушения. Мы создаем жизнь по образу и подобию своему...»

Стивен Хокинг

Моей дорогой и любимой внучке Амине с любовью и напутствием в начале ее чудесных, школьных лет:

Аминочка, в добрый путь, в Мир Знаний!

От автора

Введение

Предлагаемое учебное пособие предназначено для обучающихся в высших учебных заведениях направлений подготовки 09.03.03 «Прикладная информатика», 10.03.01 «Информационная безопасность», 27.03.02 «Управление качеством», 38.03.05 «Бизнес-информатика» и специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

В учебном пособии рассмотрена история происхождения и развития компьютерных вирусов, классификация компьютерных вирусов и вредоносного программного обеспечения глазами аналитика, с точки зрений профессионала и регулятора представлены основные виды и примеры потенциально нежелательных программ, подробно изучены программно-математическое воздействие на информацию компьютерными вирусами, пути распространения вредоносного программного обеспечения, формы организации вирусных атак, а также дана классификация антивирусных программ и определены основные методы и средства обеспечения управлением антивирусной защиты информации. Помимо этого, в учебном пособии представлен проект «WildList», основой которого является понятие «дикий вирус» и рассмотрены другие варианты реализации данного проекта. В завершающей главе учебного пособия рассматриваются вопросы, связанные с компьютерным андеграундом, а именно: дано определение

и описаны виды компьютерных преступлений, описаны компьютерная криминалистика, преступления в сфере обращения цифровой информации, рассмотрены понятие хакерства и краткая история его развития, дан обобщенный портрет вирусописателя и представлено условное разделение вирусописателей на группы.

Учебное пособие также может использоваться обучающимися других специальностей при изучении курсов (дисциплин), связанных с защитой информации.

Использование данного пособия в учебном процессе позволяет сформировать у выпускников требуемые квалификации (знания, умения и навыки), определенные учебными программами соответствующих изучаемых дисциплин.

В результате изучения основ антивирусной безопасности информации обучающийся должен:

знать

- методы и средства подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзоров по вопросам обеспечения антивирусной безопасности информации; содержание понятий «компьютерный вирус», «вредоносное программное обеспечение», «вредоносные программы»; основные угрозы антивирусной безопасности информации; классификацию вредоносного программного обеспечения; классификацию антивирусных программ; основные виды вредоносных программ и потенциально нежелательных программ; классификацию компьютерных преступлений;

уметь

- объяснять содержание обеспечения управлением антивирусной безопасности информации; обосновывать применение антивирусных средств, используемых для обеспечения антивирусной безопасности информации; охарактеризовать назначение и действие вредоносных программ;

владеть

- методами управления антивирусной защиты информации, методами анализа вопросов антивирусной безопасности информации; методами выявления компьютерных вирусов.

Полученные знания, умения и навыки при изучении основ обеспечения антивирусной безопасности, теоретические и исторические характеристики учебной дисциплины позволят успешно освоить важные и перспективные темы последующих дисциплин, понять основы междисциплинарных связей по защите ин-

формации от вирусов и основных информационных антивирусных ресурсов.

В первой главе кратко рассмотрена история происхождения и развития компьютерных вирусов, их эволюция, а также периодически возникающие эпидемии — своеобразный этногенез компьютерных вирусов.

Во второй главе дано определение понятия «компьютерный вирус», рассмотрены основы компьютерной вирусологии, представлена общепринятая классификация вредоносных компьютерных программ глазами аналитика.

В третьей главе представлена классификация вредоносного программного обеспечения по версии «Вирусной энциклопедии Касперского» (с точки зрения профессионала), а также рассмотрены пути распространения вредоносного программного обеспечения и формы организации вирусных атак.

В четвертой главе рассмотрено вредоносное программное обеспечение в виде программно-математического воздействия на информацию с точки зрения специалистов Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Программно-математическое воздействие на информацию представлено на основе методического документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

В пятой главе подробно рассмотрены основные потенциально нежелательные программы (по версии «Вирусной энциклопедии Касперского»), их своеобразный «зоопарк».

Шестая глава посвящена вопросам организации антивирусной защиты, а именно: классификация антивирусных программ, методы антивирусной защиты информации, дополнительные средства антивирусной защиты информации, функциональные модули антивирусных программ. Также в этой главе рассмотрены вопросы управления антивирусной защитой информации и приведены методы проведения испытаний программных средств на наличие компьютерных вирусов с позиций российских стандартов.

В седьмой главе дано определение понятия «дикий вирус», коротко представлены сведения о проектах «WildList», «Альянс антивирусных специалистов», связанных со сбором и обобщением информации о вирусах, атакующих компьютеры пользователей по всему миру, информация о британском журнале «Virus

Bulletin», а также рассмотрена сертификация по версии ICSA Labs.

Восьмая глава посвящена вопросам компьютерного андеграунда (компьютерные преступления, компьютерная криминалистика, компьютерные преступники, преступления в сфере обращения цифровой информации, понятие хакерства и краткая история его развития, обобщенный портрет вирусописателя).

Тематические главы учебного пособия содержат выводы, обобщающие учебный материал глав, а дидактический аппарат — контрольные вопросы и примеры (для самоконтроля).