Для ззаказа доставки данной работы воспользуйтесь поиском на сайте по ссылке: <http://www.mydisser.com/search.html>

Расследование преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ

**Год:**

2003

**Автор научной работы:**

Соловьев, Леонид Николаевич

**Ученая cтепень:**

кандидат юридических наук

**Место защиты диссертации:**

Москва

**Код cпециальности ВАК:**

12.00.09

**Специальность:**

Уголовный процесс; криминалистика и судебная экспертиза; оперативно-розыскная деятельность

**Количество cтраниц:**

275

## Оглавление диссертации кандидат юридических наук Соловьев, Леонид Николаевич

Введение.

Глава 1. Криминалистическая характеристика преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ.

§ 1. Вредоносная программа для ЭВМ: понятие, классификация.

§ 2. Наиболее распространенные способы и средства совершения и сокрытия преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ.

§ 3. Типичная обстановка совершения преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ.

§ 4. Специфические следы преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ.

§ 5. Классификации лиц, создающих, использующих и распространяющих вредоносные программы для ЭВМ.

Глава 2. Организация и планирование расследования и особенности производства первоначальных следственных действий по уголовным делам, связанным с созданием, использованием и распространением вредоносных программ для ЭВМ.

§ 1. Организация и планирование расследования преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ.

§ 2. Особенности производства первоначальных следственных действий по уголовным делам, связанным с созданием, использованием и распространением вредоносных программ для ЭВМ.

§ 3. Криминалистические аспекты предупреждения преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ.

## Введение диссертации (часть автореферата) На тему "Расследование преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ"

Актуальность исследования. Стремительное развитие научно-технического прогресса явилось одним из факторов, оказавшим влияние на существенные количественные и качественные изменения преступности. Появление новых информационных технологий не могло не привлечь внимания преступников во всем мире. Сегодня в компьютерных системах обрабатывается значительный объем разнообразной информации и с каждым днем область их использования расширяется. Скорость обработки компьютерной информации, ее гигантские объемы, относительная простота использования и обмена, предопределили компьютерным системам ведущее место в развитии современной науки и техники. В таких условияхправоохранительным органам приходится все чаще сталкиваться с преступлениями в сфере компьютерной информации.

Уголовный кодекс РФ признает преступным несанкционированный доступ к компьютерной информации (ст.272 УК РФ) и нарушение правил эксплуатации ЭВМ, системы ЭВМ и их сети1 (ст.274 УК РФ). Создание, использование и распространение вредоносных программ для ЭВМ1, а равно распространение машинных носителей с такими программами (ст.273 УК РФ) образуют самостоятельный состав преступления. По данным Главного информационного центра МВД России только за 2000 год органами внутренних дел России было зарегистрировано 800 преступлений в сфере компьютерной информации, из них связанных с созданием, использованием и распространением вредоносных программ - 172.

Основная опасность последней категории преступлений заключается в значительной области распространения вредоносных программ и массированном воздействии на компьютерную информацию. По расчетам западных специалистов, с выводами которых соглашаются и отечественные специалисты, вредоносные программы могут к 2013 году бло

1 Далее по тексту - компьютерные системы. кировать работу глобальных информационных сетей. Так при рассылке файлов по электронной почте по их данным на сегодняшний день вредоносные программы содержит каждое десятое отправление, а к 2013 году - каждое второе отправление будет содержать вредоносную программу.

Своевременное обнаружение, пресечение, раскрытие и расследование создания, использования и распространения вредоносных программ способствуют профилактике краж, мошенничества, вымогательства, хулиганства и других преступлений, включая тяжкие, такие как терроризм, диверсия.

На пресечение компьютерных преступлений, в целом, и преступлений, связанных с созданием, использованием и распространением вредоносных программ, в частности, как на одну из международных проблем, обращается внимание и на межгосударственном уровне. В мире налаживается межгосударственное взаимодействие в интересах борьбы с такими преступлениями. Подписаны и готовятся к подписанию различные многосторонние соглашения. Так, 01 июня 2001 года в Минске Российской Федерацией было подписано Соглашение о сотрудничестве государств - участников СНГ в борьбе с преступлениями в сфере компьютерной информации.

Противодействие несанкционированному воздействию вредоносных программ на компьютерную информацию представляет собой значительную техническую проблему. Она затрагивалась в работах Б.Ю.Анина, Н.Н.Безрукова, П.Ю.Белкина, В.А.Герасименко, П.Д.Зегжды, Е.В.Касперского, В.В.Мельникова, О.О.Михальского, С.Л.Островского, А.С.Першакова, А.В.Петракова, П.Л.Пилюгина, С.П.Расторгуева, А.В.Фролова, Г.В.Фролова, А.Ю.Щербакова, В.И.Ярочкина и других ученых.

В последние годы многие ученые-юристы, такие как Ю.М.Батурин, В.Б.Вехов, Ю.В.Гаврилин, А.М.Жодзишский,

1 Далее по тексту - вредоносная программа.

А.В.Касаткин, В.В.Крылов, В.Д.Курушин, В.Ю.Максимов, Е.И.Панфилова, Н.С.Полевой, А.Н.Попов, В.Ю.Рогозин, А.С.Шаталов, А.В.Шопин, Н.Г.Шурухнов и другие, обращались к проблеме борьбы с преступлениями в сфере компьютерной информации. Ведущие учебные заведения страны включили специальные главы, посвященные этой проблематике, в свои учебники.

Вместе с тем проблема расследования преступлений, связанных с созданием, использованием и распространением вредоносных программ, как правило, рассматривалась в комплексе с другими преступлениями в сфере компьютерной информации, в результате чего отчасти терялось ее своеобразие и особенности.

Обособленно от других преступлений в сфере компьютерной информации, общие вопросы и особенности расследования создания, использования и распространения вредоносных программ на диссертационном и монографическом уровнях в Российской Федерации не рассматривались.

Объектом исследования являются преступная деятельность, направленная на совершение преступлений, связанных с созданием, использованием и распространением вредоносных программ, механизм ее отражения в источниках информации, а также деятельность правоохранительных органов и спецслужб России по их расследованию.

Предметом исследования являются закономерности преступной деятельности, связанной с созданием использованием и распространением вредоносных программ, и ее раскрытия (познания) как процесса собирания, исследования и использования криминалистической информации для выявления, раскрытия, расследования и предупреждения преступлений, связанных с созданием, использованием и распространением вредоносных программ.

Целью исследования является разработка теоретических основ и практических рекомендаций по расследованию преступлений в сфере

3 компьютерной информации, связанных с созданием, использованием и распространением вредоносных программ.

Эта цель определила конкретные научные задачи исследования:

• исследование понятия вредоносной программы и других, связанных с ним, включая понятия компьютерного вируса, троянской программы и других;

• уточнение основных терминов, связанных с совершением деяний, направленных на создание, использование и распространение вредоносных программ;

• исследование и описание базовых элементов криминалистической характеристики преступлений, связанных с созданием, использованием и распространением вредоносных программ;

• исследование первоначальных ситуаций, складывающихся при расследовании уголовных дел, связанных с созданием, использованием и распространением вредоносных программ;

• исследование особенностей подготовки и производства отдельных следственных действий на первоначальном этапе расследования;

• изучение криминалистических аспектов предупреждения преступлений, связанных с созданием, использованием и распространением вредоносных программ.

Наиболее существенные научные результаты, полученные лич-g> но диссертантом, заключаются в разработке понятийного аппарата, выделении и исследовании основных элементов криминалистической характеристики преступлений, связанных с созданием, использованием и распространением вредоносных программ, их отражения и познания, а также методики расследования таких преступлений. Так, сформулированы новые и уточнены существующие понятия, связанные с созданием, использованием и распространением вредоносных программ, раскрыты базовые элементы криминалистической характеристики преступлений, связанных с созданием, использованием и распространением вредоносных программ, показаны первоначальные ситуации расследования рассматриваемых преступлений, выделены особенности подготовки и проведения следственных действий, наиболее распространенные обстоятельства, способствующие совершению преступлений рассматриваемой категории.

Основные положения, выносимые на защиту:

1) Определение вредоносной программы, под которой понимается программа для ЭВМ, наделенная функциями, выполнение которых может оказать неправомерное воздействие на средства компьютерной техники, приводящее к их уничтожению, блокированию или иному нарушению их работы, и на компьютерную информацию, приводящее к ее уничтожению, блокированию, модификации или копированию.

2) Криминалистическая классификация вредоносных программ. Вредоносные программы могут быть разделены по следующим основаниям: по способу создания, по способности к самораспространению, по наличию в них открыто декларируемых функций, по видам оказываемого воздействия, по направленности оказываемого воздействия.

По способу создания вредоносные программы классифицируются как: специально созданные, созданные путем, внесения изменений в существующие программы, и модифицированные.

Классификация вредоносных программ, основанная на способности программ к самораспространению, включает в себя два основных класса: самораспространяющиеся вредоносные программы, куда относятся компьютерные вирусы и компьютерные черви, и программные закладки. Программные закладки в свою очередь можно разделить на пять групп: осуществляющие сбор информации об информационных процессах, протекающих в компьютерной системе; обеспечивающие неправомерный доступ; наделенные деструктивными функциями; блокирующие работу средств компьютерной техники; комбинированные.

В зависимости от наличия открыто декларируемых функций вредоносные программы могут быть разделены на: троянские программы и скрытые вредоносные программы. По видам оказываемого воздействия вредоносные программы можно разделить на пять групп, куда наряду с воздействием на компьютерную информацию, должно войти и воздействие на аппаратно-технические средства ЭВМ, и возможное воздействие на здоровье человека. По направленности оказываемого воздействия: вредоносные программы делят на: направленные на индивидуально-определенный объект и ненаправленного действия.

3) Описание особенностей основных элементов криминалистической характеристики преступлений, связанных с созданием, использованием и распространением вредоносных программ: а) способов совершения преступлений, связанных с созданием, использованием и распространением вредоносных программ.

По действиям, составляющим объективную сторону совершения преступлений, все способы совершения преступлений рассматриваемой категории могут быть разделены на две группы: способы создания вредоносных программ и способы их использования и распространения.

В зависимости от совпадения мест создания вредоносной программы и мест ее последующего использования способы создания можно разделить на: создание непосредственно на месте ее использования и создание вне места ее использования, а по способу возникновения, можно выделить две группы: создание программ и внесение изменений в существующие программы.

Способы использования и распространения вредоносных программ можно разделить на две большие группы: активные и пассивные. Каждая из этих групп в свою очередь делится отдельные способы или группы способов. Основное отличие пассивных способов от активных заключается в том, действия преступника не связанны с получением доступа к компьютерной информации; б) средств создания вредоносных программ. Указанные средства можно разделить на программные и аппаратные. Программные средства делятся на четыре основные составляющие: системы программирования, специальные, отладочные и камуфлирующие (маскирующие) программные средства. Аппаратные средства создания вредоносных программ в свою очередь делятся на две группы: используемые для непосредственного создания и подготовки к распространению программ и используемые для отладки и тестирования работы создаваемой программы; в) системы элементов, характеризующих обстановку совершения преступлений, связанных с созданием, использованием и распространением вредоносных программ. Она должна включать в себя программно-технический элемент, определяющий возможность совершения тех или иных действий преступником или самой вредоносной программой в существующей программно-технической среде, а также комплексный элемент, характеризующий используемые меры защиты информации; г) следов внедрения, воздействия и функционирования вредоносных программ в компьютерных системах, следы воздействия оказываемого самим преступником на компьютерную информацию. Их можно разделить на пять основных групп: следы изменения файловой структуры, системных областей машинных носителей информации и постоянной энергонезависимой памяти; следы изменения настроек ЭВМ и отдельных программ; следы нарушения работы ЭВМ и отдельных программ; следы воздействия на системы защиты и конфиденциальность информации; иные проявления воздействия и функционирования вредоносных программ (аудио-, видеоэффекты и другие); д) лица, совершающие преступления, связанные с созданием, использованием и распространением вредоносных программ. Классификация таких лиц по целям преступного посягательства должна включать в себя особую группу - «диверсантов».

4) Классификация и характеристика типичных следственных ситуаций. Типичными ситуациями первоначального этапа расследования преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ являются три следующие следственные ситуации: а) известны лишь некоторые лица (лицо), совершившиепреступления, связанные с выявленным фактом создания, использования или распространения вредоносной программы; б) известны все лица (лицо), совершившие преступления, связанные с выявленным фактом создания, использования или распространения вредоносной программы; в) лица (лицо), совершившие преступления, связанные с выявленным фактом создания, использования или распространения вредоносной программы, неизвестны.

5) Описание особенностей подготовки и проведения отдельных следственных действий на первоначальном этапе расследования по уголовным делам о преступлениях, связанных с созданием, использованием и распространением вредоносных программ: а) основные правила поиска, фиксации и изъятия компьютерной информации и ее машинных носителей в ходе проведения следственных действий;

6) состав программных средств компьютерной техники, используемых в ходе проведения следственных действий и требования, предъявляемые к ним; в) система приемов цифровой фиксации доказательственной информации, в которую входят три основных приема фиксации цифровой информации: сохранение цифровой информации на машинном носителе; копирование существующих файлов на машинный носитель; создание образов машинных носителей информации; г) обстоятельства, способствующие совершению преступлений, связанных с созданием использованием и распространением вредоносных программ, в зависимости от способа совершения преступлений могут быть отнесены к обстоятельствам, способствующим неправомерному доступу к компьютерной информации, или обстоятельствам, способствующим непосредственно созданию, использованию и распространению вредоносных программ.

Теоретическая значимость исследования определяется тем, что оно является монографическим исследованием, в котором выделены и раскрыты основные элементы криминалистической характеристики преступлений, связанных с созданием, использованием и распространением вредоносных программ, и основные особенности методики расследования таких преступлений.

Теоретическая значимость исследования заключается также в том, что в нем сформулированы новые и уточнены существующие основные понятия, связанные с рассматривавшейся категорией преступлений, предложено авторское описание базовых элементов криминалистической характеристики указанной категории преступлений. Соискателем описаны особенности методики расследования преступлений, связанных с созданием, использованием и распространением вредоносных программ являющейся составной частью методики расследования преступлений в сфере компьютерной информации. Среди них соискателем выделены особенности организации и планирования расследования по делам, связанным с созданием, использованием и распространением вредоносных программ, а также отдельные криминалистические аспекты их предупреждения. Внесены предложения по приданию результатам предварительных исследований программ на наличие в них вредоносных функций, проведенных до возбуждения уголовного дела, доказательственного значения в уголовном процессе, а также показана целесообразность внесения в законодательство поправок, разрешающих проведение экспертных исследований до возбуждения уголовных дел без изменения их процессуального значения.

Практическая значимость исследования определяется тем, что в нем выявлены особенности методики расследования преступлений, связанных с созданием, использованием и распространением вредоносных программ, показаны возможные пути реализации в следственной и оперативно-розыскной практике данных об использовании вредоносных программах различных классов, определен состав и характеристики специальных программных средств, которые могут быть использованы в ходе проведения осмотров компьютерной информации, находящейся на машинных носителях, сформулированы рекомендации по подготовке и проведению отдельных первоначальных следственных действий с учетом особенностей рассматривавшейся категории преступлений. Соискателем разработаны методические рекомендации по проведению осмотров средств компьютерной техники и компьютерной информации, находящейся на машинных носителях.

Теоретико-методологическая основа исследования, эмпирическая основа исследовательской базы. Теоретико-методологической основой исследования являются: материалистическая диалектика; криминалистическая методология; теоретические концепции криминалистики о структуре и этапах расследования преступлений, закономерностях механизма преступлений, их отражения и познания, тактике отдельных следственных действий.

При решении поставленных задач использовался широкий круг методов научного исследования: общенаучные методы (анализ, синтез, наблюдение, сравнение, прогнозирования и др.); методы криминалистики (методы криминалистической идентификации и диагностики, криминалистического прогнозирования, организационно-структурные и тактические методы и др.).

В процессе исследования использовались положения общей теории и методологии криминалистики и судебной экспертизы, содержащиеся в работах Т.В.Аверьяновой, Р.С.Белкина, А.И.Винберга,

A.Ф.Волынского, В.Г.Корухова, З.И.Кирсанова, В.Я.Колдина,

B.В.Крылова, В.П.Лаврова, И.М.Лузгина, Н.П.Майлис, В.С.Митричева, А.С.Подшибякина, Е.Р.Россинской, Н.А.Селиванова, С.И.Цветкова, А.Р.Шляхова, Н.Г.Шурухнова, Н.П.Яблокова и других ученых.

В диссертационном исследовании были использованы данные ГИЦ МВД России и материалы 18 уголовных дел, расследовавшихся в разных регионах Российской Федерации, а также материалы информационных баз данных российских центров технической защиты информации, специализирующихся на защите средств компьютерной техники от вредоносных программ. Помимо этого в диссертационном исследовании использовались данные развития законодательной базы и подзаконных актов, регулирующих вопросы, связанные с правовой охраной и защитой компьютерной информации, материалы по вопросам, связанным с защитой компьютерной информации от воздействия вредоносных программ, данные о существующих вредоносных программах и перспективных направлениях их совершенствования, данные анализа протоколов отдельных следственных действий, в ходе которых осматривались и изымались средства компьютерной техники, теоретические положения методики расследования преступлений в сфере компьютерной информации.

Реализация и апробация полученных результатов.

Основные положения диссертационного исследования нашли отражение в опубликованных работах автора:

1) Махтаев М.Ш., Соловьев JI.H. Расследование преступлений в сфере компьютерной информации: Лекция. - М.: в/ч 33965, 2001. - 52 с.

2) Соловьев JI.H. Проведение практических занятий: следственный осмотр средств компьютерной техники / Профессиональная подготовка в учебных заведениях МВД России: Проблемы, пути их решения. - М.: ЮИ МВД РФ, 2000. - С. 43-47.

3) Соловьев JI.H. Классификация программных средств компьютерной техники, используемых при проведении следственных осмотров // Криминалистика: Актуальные вопросы теории и практики. Всероссийский круглый стол. Ростовский юридический институт МВД РФ, 15-16 июня 2000 г.-С. 192-196.

4) Махтаев М.Ш., Соловьев JI.H. Криминалистическое предупреждение преступлений в сфере компьютерной информации. // Сборник трудов адъюнктов и преподавателей. - М., 2000. - С. 88-99. Депонировано в Академии ФСБ РФ, 2000.

5) Соловьев JI.H. К вопросу о программных средствах, используемых при проведении следственных действий // Сборник научных статей преподавателей и адъюнктов. - М., 2000. - С. 124-131. Депонировано в Академии ФСБ РФ, 2000.

6) Соловьев JI.H. Способы совершения преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ // Сборник научных статей преподавателей и адъюнктов. - М., 2000. - С. 100-123. Депонировано в Академии ФСБ РФ, 2000.

Основные положения, нашедшие отражение в опубликованных работах соискателя, внедрены в практику деятельности Следственного управления ФСБ РФ.

Результаты исследования внедрены в учебный процесс Академии ФСБ РФ, Юридического института МВД РФ, МГИМО (Университета) МИД РФ.

Обоснование структуры диссертации. Структура диссертации обусловлена задачами исследования, а также современным состоянием научной разработки рассматриваемых вопросов. Работа состоит из введения, двух глав, включающих в себя восемь параграфов, заключения и приложений.

## Заключение диссертации по теме "Уголовный процесс; криминалистика и судебная экспертиза; оперативно-розыскная деятельность", Соловьев, Леонид Николаевич

Заключение

Проведенное исследование дает основание для формулирования следующих основных выводов, предложений и рекомендаций:

1. Важность правильного и полного определения понятия вредоносной программы обуславливается тремя группами факторов: связанными с увеличением числа преступлений, в которых используются вредоносные программы; связанными с увеличением числа создаваемых и распространяющихся вредоносных программ и расширением их вредоносных функций; правовыми факторами, связанными с определением соотношения программ для ЭВМ и вредоносных программ.

Учитывая понятие программы для ЭВМ, даваемое в законодательстве, а также современный уровень технического развития программ, которые могут быть отнесены к вредоносным, вредоносную программу можно определить как программу для ЭВМ, наделенную функциями, выполнение которых может оказать неправомерное воздействие на средства компьютерной техники, приводящее к их уничтожению, блокированию или иному нарушению их работы, и на компьютерную информацию, приводящее к ее уничтожению, блокированию, модификации или копированию.

2. Непосредственно связанным с понятием вредоносной программы, является понятие электронной вычислительной машины (ЭВМ). Под ЭВМ понимается комплекс взаимосвязанных и взаимодействующих через определенное программное обеспечение электронных и электронно-механических устройств, обеспечивающий протекание информационных процессов. Программное обеспечение можно определить как совокупность программных средств компьютерной техники, используемых для управления функционированием конкретной ЭВМ, системой ЭВМ или их сетью и информационными процессами, протекающими в них.

3. Вопросы, связанные с созданием вредоносных программ и внесением изменений в существующие программы, заведомо приводящим к указанным в уголовном законе последствиям, в действующем уголовном законодательстве не достаточно проработаны. В частности формулировка уголовного закона позволяет в целом ряде случаев избежать уголовной ответственности лицам, модифицировавшим существующие вредоносные программы.

4. Все существующие вредоносные программы можно разделить на специально созданные, созданные путем, внесения изменений в существующие программы, и модифицированные.

Под созданием вредоносной программы следует понимать творческую деятельность, направленную на создание качественно новой программы, заведомо наделенной функциями, выполнение которых может оказать неправомерное воздействие на средства компьютерной техники.

Под программами, созданными путем внесения изменений в существующие программы, следует понимать вредоносные программы, созданные путем внесения любых изменений в существующие программы при условии, что эти изменения значительно качественно изменили существующую программу.

Под модифицированной вредоносной программой следует понимать вредоносную программу, в которую внесены любые изменения, при условии, что эти изменения значительно качественно не изменили ее и она не изменила своих функций, выполнение которых оказывает неправомерное воздействие на компьютерную информацию и средства компьютерной техники.

5. Вредоносные программы могут быть классифицированы и по другим основаниям, основными из которых являются классификации по способности к самораспространению, по наличию в них открыто декларируемых функций, по видам оказываемого воздействия, по направленности оказываемого воздействия.

По способности вредоносных программ к самораспространению их можно разделить на два класса: самораспространяющиеся вредоносные программы (компьютерные вирусы и компьютерные черви) и программные закладки. Все существующие программные закладки составляют пять групп: осуществляющие сбор информации об информационных процессах, протекающих в компьютерной системе; обеспечивающие неправомерный доступ; наделенные деструктивными функциями; блокирующие работу средств компьютерной техники; комбинированные. В зависимости от наличия открыто декларируемых функций вредоносные программы могут быть разделены на: троянские программы и скрытые вредоносные программы. На основе прогнозов дальнейшего развития и современных данных о видах оказываемого воздействия, вредоносные программы можно разделить на пять групп, куда наряду с воздействием на компьютерную информацию, должно войти и воздействие на аппаратно-технические средства ЭВМ, и возможное воздействие на здоровье человека. По направленности оказываемого воздействия вредоносные программы делят на: направленные на индивидуально-определенный объект и ненаправленного действия.

6. Система свойств файлов, ранее приводившаяся в литературе, должна быть уточнена путем внесения в нее ряда изменений, основным из которых является включение такого элемента системы как физическое размещение файла на машинном носителе информации. Это свойство определяет не размещение файла в файловой структуре машинного носителя информации, а именно физическое размещение намагниченных участков рабочих поверхностей машинных носителей информации, содержащих компоненты файла, с которыми он связан, в которых располагается его физический объем.

7. Основными элементами криминалистической характеристики преступлений, связанных с созданием, использованием и распространением вредоносных программ являются: способы совершения и сокрытия преступлений; средства совершения преступлений; типичная обстановка совершения преступлений; следы преступлений; данные о личностипреступника.

8. В связи со значительными различиями в действиях преступника, выполняющего объективную сторону преступления, все способы совершения преступлений рассматриваемой категории могут быть разделены на две группы: создание вредоносных программ и их использование и распространение.

По способу возникновения вредоносных программ можно выделить две группы способов создания вредоносных программ: создание и внесение изменений в существующие программы. В зависимости от совпадения мест создания вредоносной программы и мест ее последующего использования способы создания можно разделить на: создание непосредственно на месте ее использования и создание вне места ее использования.

Способы использования и распространения вредоносных программ можно разделить на активные и пассивные. Основное отличие пассивных способов от активных заключается в том, действия преступника не связанны с получением доступа к компьютерной информации.

9. Среди средств создания, использования и распространения вредоносных программ в отдельную группу необходимо выделить средства их создания. На сегодняшний день можно определить четыре основные составляющие программных средств создания вредоносных программ: системы программирования, специальные, отладочные и камуфлирующие (маскирующие) программные средства. Аппаратные средства создания вредоносных программ в свою очередь могут быть разделены на две группы: средства, используемые для непосредственного создания и подготовки к распространению программ, и средства, используемые для отладки и тестирования работы создаваемой программы.

10. Система элементов, характеризующих обстановку совершения преступлений, связанных с созданием, использованием и распространением вредоносных программ, должна включать в себя программно-технический элемент, определяющий возможность совершения тех или иных действий преступником или самой вредоносной программой в существующей программно-технической среде, а также комплексный элемент, характеризующий используемые меры защиты информации.

11. Следы внедрения, воздействия и функционирования вредоносных программ в компьютерных системах, следы воздействия оказываемого самим преступником на компьютерную информацию можно разделить на пять основных групп: следы изменения файловой структуры, системных областей машинных носителей информации и постоянной энергонезависимой памяти; следы изменения настроек ЭВМ и отдельных программ; следы нарушения работы ЭВМ и отдельных программ; следы воздействия на системы защиты и конфиденциальность информации; иные проявления воздействия и функционирования вредоносных программ (аудио-, видеоэффекты и другие).

12. Классификация лиц, совершающих преступления в сфере компьютерной информации, должна включать в себя особую группу - «диверсантов». Основным характеризующим признаком этой группы является направленность действий преступников на достижение определенной цели - подрыв экономической безопасности и обороноспособности страны, и обусловленное ею воздействие, направленное на определенные системы, обладающие рядом специфических свойств.

13. На первоначальном этапе расследования преступлений, связанных с созданием, использованием и распространением вредоносных программ можно выделить три наиболее вероятных типичных следственных ситуации:

1) Известны лишь некоторые лица (лицо), совершившие преступления, связанные с выявленным фактом создания, использования или распространения вредоносной программы.

2) Известны все лица (лицо), совершившие преступления, связанные с выявленным фактом создания, использования или распространения вредоносной программы.

3) Лица (лицо), совершившие преступления, связанные с выявленным фактом создания, использования или распространения вредоносной программы, неизвестны.

14. К общим версиям по делам рассматриваемой категории можно отнести следующие версии:

1) Совершено преступление, связанное с созданием вредоносных программ;

2) Совершено преступление, связанное с использованием вредоносных программ;

3) Совершено преступление, связанное с распространением вредоносных программ или машинных носителей с такими программами;

4) Совершено преступление в сфере компьютерной информации без использования вредоносных программ;

5) Совершено преступление, не относящееся к преступлениям в сфере компьютерной информации;

6) Преступления совершено не было, при этом заявитель добросовестно заблуждается;

7) Заявление о преступлении ложное.

Среди частных версий особо следует выделить версии о характере и реальном размере нанесенного ущерба, версии о лицах, причастных к совершению преступления, включая лиц, создавших, внедривших, использовавших и распространявших вредоносные программы, а также версии о возможных направлениях распространения вредоносных программ и области возможного поражения ими.

15. Классификация программных средств, используемых в ходе проведения следственных действий, по основным направлениям их использования включает в себя пять групп: для получения информации о входящих в состав компьютерных систем и подключенных к ним устройствам, включая их техническое состояние, настройки и конфигурацию; для получения информации о файловой структуре машинных носителей информации; для выявления внедренных и функционирующих в компьютерной системе вредоносных программ; для получения информации о функционирующих на момент осмотра программах, находящихся в оперативной памяти ЭВМ, о содержимом буфера памяти ЭВМ; для определения настроек программ, просмотра и иного воспроизведения содержимого файлов.

16. Проблемы проведения судебной компьютерно-технической экспертизы и иных исследований, связанных со специфическими объектами, по делам рассматриваемой категории имеет огромное значение и требует самостоятельной научной проработки.

17. Без предварительного решения вопроса об отнесении какой-либо программы к категории вредоносных, нельзя решить вопрос о возбуждении уголовного дела по признакам ст. 273 УК РФ. Препятствием к назначению экспертизы для решения вопроса об относимости программы к вредоносным является невозможность назначения экспертизы до возбуждения уголовного дела, в то время как дело нельзя возбудить без решения этого вопроса. Эту общую коллизию, характерную не только для преступлений рассматриваемой категории, предлагается решить одним из двух способов: 1) предать результатам предварительных исследований значение источника доказательств, хотя бы на стадии возбуждения уголовного дела; 2) разрешить, в случаях, когда принятие решения о возбуждении уголовного дела невозможно без производства экспертизы, проведение экспертиз до возбуждения уголовного дела.

18. В настоящее время можно говорить о сложившейся в криминалистике системе приемов цифровой фиксации доказательственной информации. В эту систему должны войти три основных приема фиксации цифровой информации: сохранение цифровой информации на машинном носителе (цифровая фотография, звукозапись, цифровая запись данных различных приборов и т.д.); копирование существующих файлов на машинный носитель информации; создание образов машинных носителей информации.

19. Расследование любого преступления, в том числе и преступления, связанного с созданием, использованием распространением вредоносных программ нельзя считать завершенным, до тех пор, пока не будут выявлены и устранены все обстоятельства, способствующие их совершению. С учетом возможных способов совершения преступлений рассматриваемой категории, для их предупреждения могут иметь значение как обстоятельства, способствующие неправомерному доступу, так и обстоятельства, способствующие непосредственно созданию, использованию и распространению вредоносных программ.

Таким образом, проведенное исследование показало, что проблемы расследования преступлений, связанных с созданием, использованием и распространением вредоносных программ, можно отнести к числу сложных и слабо разработанных. Отдельные положения и выводы диссертационного исследования в силу новизны самой проблемы и малого объема эмпирического материала в этой области в известной мере дискуссионны. Правильность и объективность теоретических положений, а также выводов и предложений, сформулированных в рамках диссертационного исследования может быть доказана только практикой, которая безусловно скорректирует, разовьет и обогатит полученные результаты.

## Список литературы диссертационного исследования кандидат юридических наук Соловьев, Леонид Николаевич, 2003 год

1. Нормативно-правовые акты

2. Конституция Российской Федерации. М.: Юридическая литература, 1993.-96 с.

3. Уголовный кодекс Российской Федерации // Собрание законодательства Российской Федерации, 17 июня 1996 года, № 25, ст.2954.

4. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 года № 174-ФЗ // Российская газета, 22 декабря 2001 года.

5. Соглашение о сотрудничестве государств участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 01 июня 2001 года).

6. Доктрина информационной безопасности Российской Федерации от 09 сентября 2000 года № ПР-1895 // Российская газета, 28 сентября 2000 года, № 187.

7. Закон Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации от 13 февраля 1992 г., № 7, ст. 300.

8. Федеральный закон Российской Федерации от 29 декабря 1994 года № 77-ФЗ «Об обязательном экземпляре документов» // Собрании законодательства Российской Федерации от 2 января 1995 года, № 1, ст. 1.

9. Федеральный закон Российской Федерации от 20.02.1995 года № 24-ФЗ «Об информации, информатизации и защите информации» // Собрание законодательства Российской Федерации, 1995, № 8, ст.609.

10. Федеральный закон Российской Федерации от 03.04.1995 года № 40-ФЗ «Об органах федеральной службы безопасности в Российский Федерации» // Собрание законодательства РФ, № 15, ст. 1269.

11. Федеральный закон Российской Федерации от 12.08.1995 года №114-ФЗ «Об оперативно-розыскной деятельности» // Собрание законодательства РФ, 1995, № 33, ст.3349.

12. Федеральный закон Российской Федерации от 04.07.1996 года № 85-ФЗ «Об участии в международном информационном обмене» // Собрание законодательства Российской Федерации от 8 июля 1996 года, №28, ст. 3347.

13. Федеральный закон Российской Федерации от 25.07.1998 года jsfo 130-ФЗ «О борьбе с терроризмом»//Ведомости Федерального Собрания Российской Федерации, 1998, № 24.

14. Федеральный закон Российской Федерации от 31 мая 2001 года № 73-Ф3 «О государственной судебно-экспертной деятельности в Российской Федерации» // Собрание законодательства Российской Федерации, 2001, № 23, ст.2291.

15. Федеральный закон Российской Федерации от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности» // Собрание законодательства Российской Федерации, 2002, № 30, ст.3031.

16. Закон Российской Федерации от 5 марта 1992 года № 2446/1-1 «О безопасности» // Ведомости Совета народных депутатов и Верховного Совета РФ, 1992. № 15. ст.769.

17. Закон Российской Федерации от 23 сентября 1992 года № 3526-1 «О правовой охране топологий интегральных микросхем» // Ведомости Съезда Народных Депутатов Российской Федерации и Верховного Совета Российской Федерации от 22 октября 1992 г., № 42, ст.2328

18. Указ Президента Российской Федерации от 14 июня 94 года № 1226 «О неотложных мерах по защите населения от бандитизма и иных проявлений организованной преступности //Российская газета, 17 июня 1994 года.

19. Указ Президента Российской Федерации от 7.03.96 г. № 338 «О мерах по усилению борьбы с терроризмом» // Собрание законодательства РФ, 1996, ст. 1027.

20. Указ Президента Российской Федерации от 10 января 2000 года № 24 «О Концепции национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации, 2000, № 2, ст. 170.

21. Постановление Центральной избирательной комиссии Российской Федерации от 09 июля 1999 года № 7/41-III «Об утверждении Положения об обеспечении информационной безопасности государственной автоматизированной системы Российской Федерации «Выборы».

22. Правовое руководство ЮНСИТРАЛ по электронному переводу средств (подготовлено секретариатом Комиссии Организации Объединенных Наций по праву международной торговли, Нью-Йорк, 1987 г.)

23. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. 10 с.

24. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

25. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

26. ГОСТ 6.10.4-84 Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемыми средствами вычислительной техники.

27. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. -М.: Воениздат, 1992.

28. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Концепция защиты средств вычислительной техники и автоматизированных от несанкционированного доступа к информации. М.: Воениздат, 1992.

29. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М.: Воениздат, 1992.

30. Уголовное дело № 016496 по обвинению Лукьянова Р.В. в совершении преступления, предусмотренного ч.1 ст.273 УК РФ.

31. Уголовное дело № 176709 по обвинению Флягина А.А. в совершении преступления, предусмотренного ч.1 ст.273 УК РФ.

32. Уголовное дело № 530690 по обвинению Гугняева М.Г. в совершении преступления, предусмотренного ч.1 ст.273 УК РФ.

33. Уголовное дело № 60-99-05 по обвинению Горбунова В.Ю., Дунаевой М.Р., Чекалина В.В. в совершении преступления, предусмотренного ч.З ст. 30 УК РФ, ч.2 ст.272 УК РФ.

34. Уголовное дело № 6609 по обвинению Шрафи Абед Маттера и Кайед Фади Камеля, в преступлениях, предусмотренных п.«б» ч.З ст. 165 УК РФ, ч.2 ст.35, ч.1 ст. 183 УК РФ, ч.2 ст.35, ч.2 ст. 183 УК РФ, ч.2 ст.272 УК РФ, ч.2 ст.35, п. «б» ч.2 ст.171 УК РФ.

35. Уголовное дело № 73129 по обвинению Турунина Н.К. и Курдиной Е.В. в совершении преступления, предусмотренного ч.2 ст.272 УК РФ.

36. Уголовное дело № 97143995 по обвинению Лопатина А.Н. и Макеева А.Н. в совершении преступлений, предусмотренных ч.2 ст.272 УК РФ и п.«а» ч.З ст. 165 УК РФ.

37. Уголовное дело № 844498 по обвинению Л.В. и Л.П. в совершении преступлений, предусмотренных ч.2 ст.35 УК РФ, чЛ. ст.273 УК РФ, ч.2. ст. 146 УК РФ.

38. Уголовное дело № 77772 по обвинению П. в совершении преступлений, предусмотренных ч. 1 ст. 327 УК РФ, ч. 1 ст.183 УК РФ, ч.2. ст. 183 УК РФ, чЛ. ст.273 УК РФ, ч.2 ст. 272 УК РФ, ч.З ст.165 УК РФ.

39. Уголовное дело № 010317 по обвинению Ч. в совершении преступлений, предусмотренных ч.2 ст. 272 УК РФ, п. «б» ч.З ст. 159 УК РФ, и 3. в совершении преступления, предусмотренного п. «б» ч.З ст. 159 УК РФ.

40. Уголовное дело № 011678 по обвинению Ф. в совершении преступлений, предусмотренных ст. 242 и ч.2 ст.272 УК РФ.

41. Уголовное дело № 444800 по обвинению П. в совершении преступления, предусмотренного ч. 2 ст.272 УК РФ, чЛ ст.165 УК РФ.

42. Уголовное дело № 73129 по обвинению Т. и К. в совершении преступления предусмотренного ч.2 ст. 272 УК РФ.

43. Уголовное дело № 9010076 по обвинению М. и Н. в совершении преступления, предусмотренного ч.2 ст. 272 УК РФ, чЛ и ч.2 ст. 183 УК РФ.

44. Уголовное дело № 9983239 по обвинению Ш. и других по ч. 2 ст. 272 УК РФ.

45. Уголовное дело № 444800 по обвинению П. в совершении преступлений, предусмотренных ч.2 ст.272 УК РФ, чЛ ст.165 УК РФ.

46. Уголовное дело № 1010055 по обвинению X. в совершении преступлений, предусмотренных ч.2 ст.272 УК РФ, ч.1 ст. 165 УК РФ.1. Открытая литература

47. Аванесов Г.А. Теория и методология криминологического прогнозирования. М.: Юридическая литература, 1972. - 334 с.

48. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Российская Е.Р. Криминалистика. Учебник для вузов. / Под ред. Заслуженного деятеля науки Российской Федерации, профессора Р.С.Белкина. М.: Издательская группа НОРМА-ИНФРА-М, 1999. - 990 с.

49. Агапов А.Б. Основы федерального информационного права России. М.: Экономика. 1995. - 145 с.

50. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Пер. с англ. М.: Мир, 1999.-351 с.

51. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. М.: ООО Издательство «Юр-литинформ», 2001. - 152 с.

52. Анин Б.Ю. Защита компьютерной информации. СПб.: БХВ -Санкт-Петербург, 2000. - 384 с.

53. Астапкина С.М. Тактика обыска и выемки: Лекция. М.: Академия МВД СССР, 1989.-20 с.

54. Баев О.Я. Основы криминалистики: курс лекций. М.: Экзамен, 2001.-288 с.

55. Баев О.Я. Содержание и формы криминалистической тактики. Воронеж: Изд-во Воронежского университета, 1975. - 59 с.

56. Баев О.Я. Тактика следственных действий: Учебное пособие. Воронеж: Изд-во Воронежского университета, 1992. - 205 с.

57. Баранов А.К., Цветков С.И. Компьютерные системы поддержки принятия следователем тактических решений. М.: Академия МВД РФ, 1992.- 110 с.

58. Батурин Ю.М. Проблемы компьютерного права. М.: Юридическая литература, 1991.-271 с.

59. Батурин Ю.М., Жодзишский A.M. Компьютерная преступность и компьютерная безопасность. М.: Юридическая литература, 1991. -160 с.

60. Безруков Н.Н. Классификация компьютерных вирусов MS DOS и методы защиты от них. М.: СП «1СЕ», 1990. - 48 с.

61. Безруков Н.Н. Компьютерная вирусология: Справочное руководство. Киев: Украинская советская энциклопедия, 1991. - 416 с.

62. Безруков Н.Н. Компьютерные вирусы. М.: Наука, 1991. - 158 с.

63. Белкин П.Ю., Михальский О.О., Першаков А.С. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учебное пособие для вузов. М.: Радио и связь, 1999. - 168 с.

64. Белкин Р.С. Азбука следователя. М.: Юридическая литература, 1997. - 109 с.

65. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М.: Издательство НОРМА (Издательская группа НОРМА-ИНФРА\*М), 2001. - 240 с.

66. Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории. М.: Юристъ, 1987. - 270 с.

67. Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. От теории к практике. М.: Юристъ, 1988. - 302 с.

68. Белкин Р.С. Криминалистика: Учебный словарь-справочник. М.: Юристъ, 1999.-266 с.

69. Белкин Р.С. Курс криминалистики: Учебное пособие для вузов. -М.: ЮНИТИ-ДАНА, Закон и право, 2001.-837 с.

70. Белкин Р.С. Очерки криминалистической тактики: Учебное пособие. Волгоград: ВСШ МВД РФ, 1993. - 200 с.

71. Божкова Н.Р., Власенко В.Г., Комиссаров В.И. Следственная (криминалистическая) тактика. Учебное пособие. Часть 1. Саратов: Саратовская государственная академия права, 1996. - 126 с.

72. Васильев А.Н. Следственная тактика. М.: Юридическая литература, 1976.- 196 с.

73. Васильев А.Н. Тактика отдельных следственных действий. М.: Юридическая литература, 1981. - 112 с.

74. Васильев А.Н., Яблоков Н.П. Предмет, система и теоретические основы криминалистики. М.: Изд-во Московского университета, 1984.- 143 с.

75. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия / Под ред. акад. Б.П.Смагоринского. М.: Право и Закон, 1996.- 182 с.

76. Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: Дис. . канд. юрид. наук: 12.00.09. Волгоград, 1995. - 282 с.

77. Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: Ав-тореф. дис. . канд. юрид. наук: 12.00.09. Волгоград, 1995. - 27 с.

78. Взаимодействие следователя и эксперта-криминалиста при производстве следственных действий: Учебное пособие. / Под ред. И.Н.Кожевникова. М.: ЭКЦ МВД РФ, 1995. - 134 с.

79. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: ООО Издательство «Юрлитинформ», 2002. - 496 с.

80. Волчецкая Т.С. Моделирование криминальных и следственных ситуаций: Учебное пособие. Калининград: Калининградский государственный университет, 1994. - 43 с.

81. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации. Автореферат диссертации канд. юрид. наук. Москва, 2000. 24 с.

82. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации: Учебное пособие / Под ред. профессора Н.Г.Шурухнова. М.: ЮИ МВД РФ, Книжный мир, 2001. - 88 с.

83. Гаврилов О.А. Компьютерные технологии в правоохранительной деятельности: Учебное пособие. М.: Издательская группа НОР-МА-ИНФРА-М, 1999. - 108 с.

84. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. М.: МИФИ, 1995. - 365 с.

85. Галатенко В.А. Информационная безопасность: практический подход. М.: Наука, 1998. - 301 с.

86. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.: Кн.1.- М.: Энергоатомиздат, 1994. -400 с.

87. Герасименко В.А., Милюк А.А. Основы защиты информации. М.: Московский государственный инженерно-физический институт (Технологический университет), 1997. - 538 с.

88. Глушков Н.В., Тройнин В.И., Тямкин А.В. Основы предупреждения и раскрытия преступлений подразделениями вневедомственной охраны: Учебное пособие. Воронеж: BBLLI МВД России, 1996. - 86 с.

89. Горяинов К.К., Кваша Ю.Ф., Сурков К.В. Федеральный закон «Об оперативно-розыскной деятельности»: Комментарий. М.: Новый юрист, 1997. - 155 с.

90. Гульев И.А. Создаем вирус и антивирус. М.: ДМК, 1999. - 304 с.

91. Гунтарь К.Ю., Гунтарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. Киев: «Корншчук», 2000. - 152 с.

92. Девис П., Льюис Б. Компьютерная безопасность для «чайников».: Пер. с англ. К.: Диалектика, 1997. - 272 с.

93. Домашев А.В., Попов В.О., Правиков Д.И., Прокофьев И.В., Щербаков А.Ю. Программирование алгоритмов защиты информации: Учебное пособие. М.: «Нолидж», 2000. - 288 с.

94. Драпкин Л.Я. Основы теории следственных ситуаций.- Свердловск: Изд-во Уральского университета, 1987. 163 с.

95. Драпкин Л.Я., Долинин В.Н. Тактика отдельных следственных действий. Екатеринбург: ЕВШ МВД РФ, 1994. - 31 с.

96. Дубровинская Л.П., Лузгин И.М. Планирование расследования: Учебное пособие. М.: ВШ МВД СССР, 1972. - 54 с.

97. Ермолович В.Ф. Криминалистическая характеристика преступлений. Мн.: Амалфея, 2001. - 304 с.

98. Защита информации в компьютерных системах. Под ред. Э.М.Шмакова СПб.: Изд-во Санкт-Петербургского государственного технологического университета, 1993. - 100 с.

99. Зинин A.M., Майлис Н.П. Судебная экспертиза. Учебник. М.: Право и закон; Юрайт-Издат, 2002. - 320 с.

100. Зорин Г.А. Использование криминалистических игр, инверсий, эффектов и тактических ловушек при расследовании, обвинении и защите по уголовным делам. Учебно-практическое пособие. М.: ООО Издательство «Юрлитинформ», 2002. - 360 с.

101. Зорин Г.А. Криминалистическая методология.- Мн.: Амалфея, 2000. 608 с.

102. Зорин Г.А. Руководство по тактике допроса. Учебно-практическое пособие. М.: ООО Издательство «Юрлитинформ», 2001. - 320 с.

103. Информатика в терминах и определениях российского законодательства. Под ред. В.А.Никитова. М.: Славянский диалог, 2000. -431 с.

104. Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: Автореф. дис. . канд. юрид. наук: 12.00.09 / Юридический институт. М., 1997. -23 с.

105. Касперски Крис Техника и философия хакерских атак, М.: Со-лон-Р, 1999. - 272 с.

106. Касперский Е.В. Компьютерные вирусы в MS DOS. М.: ЭДЭЛЬ, 1992.- 176 с.

107. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. М.: СК Пресс, 1998. - 288 с.

108. Катков С.А., Собецкий И.В., Федоров A.J1. Подготовка и назначение программно-технической экспертизы. Методические рекомендации // Бюллетень ГСУ России. № 4, 1995.

109. Кирсанов З.И. Криминалистические учения о механизме преступления и его отражении. Лекция. М.: Войсковая часть 33965, 1994. -28 с.

110. Кирсанов З.И. Теоретические основы криминалистики: Учебное пособие. М.: Войсковая часть 33965, 1998. - 201 с.

111. Коваль И. Как написать компьютерный вирус. Практика программирования на ассемблере. СПб.: Символ-Плюс, 2000. - 192 с.

112. Кокурин Г.А. Криминалистические и оперативно-розыскные основы поисковой деятельности в процессе раскрытия и расследования преступлений: Монография. Екатеринбург: Уральский юридический институт МВД России, 1999. - 213 с.

113. Колкутин В.В., Зосимов С.М., Пустовалов Л.В., Харламов С.Г., Аксенов С.А. Судебные экспертизы. М.: ООО Издательство «Юрли-тинформ», 2001. - 288 с.

114. Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. профессор А.В.Наумов. М.: Юристь, 1996. - 824 с.

115. Комментарий к Уголовно-процессуальному кодексу РСФСР. М.: Издательство «Спарк», 1995. - 613 с.

116. Копылов В.А. Информационное право: Учебное пособие. М.: Юристь, 1997. - 472 с.

117. Кореневский Ю.В., Токарева М.Е. Использование результатов оперативно-розыскной деятельности в доказывании по уголовным делам. Методическое пособие. М.: ООО Издательство «Юрлитин-форм», 2000. - 152 с.

118. Корухов Ю.Г. Криминалистическая диагностика при расследовании преступлений. Научно-практическое пособие. М.: Издательская группа НОРМА-ИНФРА-М, 1998. - 288 с.

119. Криминалистика: Краткая энциклопедия / Авт. сост. Р.С.Белкин.-М.: Большая Российская энциклопедия, 1993. 111 с.

120. Криминалистика: Учебник / Отв. ред. Н.П.Яблоков. М.: Юристь, 2001.-718 с.

121. Криминалистика: Учебник / Под ред. В.А.Образцова. М.: Юристъ, 1999.-735 с.

122. Криминалистика: Учебник / Под ред. И.Ф.Пантелеева, Н.А.Селиванова. М.: Юридическая литература, 1993. - 592 с.

123. Криминалистика: Учебник для вузов. / Под ред. И.Ф.Герасимова, Л.Я.Драпкина. М.: Высшая школа, 2000. - 672 с.

124. Криминалистика: Учебник для вузов/ А.Ф.Волынский, Т.В.Аверьянова, И.Л.Александрова и др.; Под ред. проф. А.Ф.Волынского.- М.: Закон и право, ЮНИТИ-ДАНА, 1999. -615 с.

125. Криминалистический словарь: Пер.: с нем. М.: Юридическая литература, 1993. - 192 с.

126. Криминалистическое обеспечение деятельности криминальной милиции и органов предварительного расследования / Под ред. проф. Т.В.Аверьяновой и проф. Р.С.Белкина. М.: Новый юрист, 1997.400 с.

127. Крылов В.В. Информационные компьютерные преступления. М.: Издательская группа ИНФРА-М-НОРМА, 1997. - 285 с.

128. Крылов В.В. Расследование преступлений в сфере информации.-М.: Издательство «Городец», 1998. 264 с.

129. Курс криминалистики. Общая часть. / Отв. ред. В.Е.Корноухов. -М.: Юристъ, 2000. 784 с.

130. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. М.: Новый Юрист, 1998. 256 с.

131. Левин М. Как стать хакером: Справочник. М.: Оверлей, 2001.326 с.

132. Левин М. Методы хакерских атак. М.: Познавательная книга плюс, 2001.-224 с.

133. Левин М. Руководство для хакеров. М.: Оверлей, 2001. - 416 с.

134. Левин М. Руководство для хакеров: Книга вторая: Электронные корсары. М.: Оверлей, 2001. - 416 с.

135. Левин М. Секреты компьютерных взломщиков: Крэкинг. М.: Познавательная книга плюс, 2001. - 224 с.

136. Леонтьев Б. Хакеры & Internet. М.: Познавательная книга, 1998. -430 с.

137. Леонтьев Б. Хакеры, взломщики и другие информационные убийцы. М.: Познавательная книга, 1999. - 192 с.

138. Леонтьев Б. Хакинг без секретов. М.: Познавательная книга Плюс, 2000. - 736 с.

139. Малахов В.П. Логика построения следственных версий: Лекция.-М.: МЮИ, 1996.-26 с.

140. Мафтик С. Механизмы защиты в сетях ЭВМ: Пер. с англ. М.: Мир. - 1993.-216 с.

141. Махтаев М.Ш. Основы теории криминалистического предупреждения преступлений: Монография. М.: Раритет, 2001. - 272 с.

142. Медведовский И.Д., Семенов П.В., Платонов В.В. Атака через INTERNET / Под науч. ред. проф. П.Д.Зегжды. СПб: Мир и семья-95, 1997.-296 с.

143. Мельников В.В. Защита информации в компьютерных системах.-М.: Финансы и статистика; Электроинформ, 1997. 368 с.

144. Мячев А.А. Персональные ЭВМ: краткий энциклопедический справочник. М.: Финансы и статистика, 1992. - 384 с.

145. Нанс Б. Компьютерные сети: Пер. с англ. М.: Восточная Книжная Компания, 1996.-400 с.

146. Образцов В.А. Выявление и изобличение преступника. М.: Юристъ, 1997.-333 с.

147. Основы криминалистики: Учебное пособие для вузов. / Под ред. И.Ф.Пантелеева. М.: ВЮЗИ, 1988. - 357 с.

148. Пантелеев И.Ф. Теоретические проблемы советской криминалистики: Учебное пособие. М.: ВЮЗИ, 1980. - 96 с.

149. Петраков А.В. Введение в электронную почту. М.: Финансы и статистика, 1993. - 208 с.

150. Петраков А.В. Защита и охрана личности, собственности, информации: Справочное пособие. М.: Радио и связь, 1997. - 320 с.

151. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. М.: ДМК, 2000. - 448 с.

152. Петровский А., Леонтьев Б. Эффективный хакинг для начинающих и не только. /Кратко, доступно, просто/. М.: Познавательная книга плюс, 1999. - 192 с.

153. Пилюгин П.Л. Компьютерные вирусы. Курс лекций. М.: Войсковая часть 33965, 1991. - 108 с.

154. Пилюгин П.Л. Общие вопросы защиты вычислительных систем и особенности защиты персональных компьютеров. Курс лекций. -М.: Войсковая часть 33965, 1997. 84 с.

155. Подшибякин А.С. Криминалистическое прогнозирование: методологические аспекты. М.: РИО Академии ФСБ РФ, 1996. - 45 с.

156. Подшибякин А.С. Холодное оружие. Криминалистическое учение. -М.: Учебно-консультационный центр «ЮрИнфоР», 1997. 240 с.

157. Пособие для следователя: Расследование преступлений повышенной общественной опасности. Коллектив авторов М.: Лига Разум, 1999.-508 с.

158. Правовая информатика и кибернетика. Учебник / Под ред. Н.С.Полевого. М.: Юридическая литература, 1993. - 528 с.

159. Приходько А.Я. Информационная безопасность в событиях и фактах. Серия «Информационная безопасность». М.: СИНТЕГ, 2001. -260 с.

160. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учебное пособие для вузов. М.: Радио и связь, 2000. - 168 с.

161. Ракитов А.И. Философия компьютерной революции. М.: Политиздат, 1991.-286 с.

162. Расследование неправомерного доступа к компьютерной информации / Под ред. Н.Г.Шурухнова. М.: Издательство «Щит-М», 1999.-254 с.

163. Рогозин В.Ю. Особенности расследования и предупреждения преступлений в сфере компьютерной информации: Автореферат дис. канд. юрид. наук. Волгоград, 1998. 21 с.

164. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях/ Под ред. В.Ф. Шаньгина М.: Радио и связь, 1999.- 328 с.

165. Российская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. М.: Право и закон, 2001. - 416 с.

166. Руководство для следователей / Под ред. Н.А.Селиванова, В.А.Снеткова. М.: ИНФРА-М, 1997. - 732 с.

167. Рыкунов В.И. Механизм управления (Монография). М.: РЭА им. Г.В.Плеханова, 1999. - 168 с.

168. Сахнова Т.В. Судебная экспертиза. М.: Городец, 2000. - 368 с.

169. Селиванов Н.А. Советская криминалистика: Система понятий. М.: Юридическая литература, 1982. - 150 с.

170. Симкин JI.C. Программы для ЭВМ: правовая охрана (правовые средства против компьютерного пиратства). М.: Издательство «Городец», 1998.-208 с.

171. Следственная тактика: Учебное пособие. / Отв. ред. И.Ф.Пантелеев. М.: ВЮЗИ, 1982. - 77 с.

172. Следственные действия: Криминалистические рекомендации. Типовые образцы документов. / Под ред. В.А.Образцова. М.: Юристъ, 1999. - 499 с.

173. Смирнов М.П. Комментарий оперативно-розыскного законодательства РФ и зарубежных стран. Учебное пособие. М.: Издательство «Экзамен», 2002. - 544 с.

174. Соколов А.В., Степанюк О.М. Методы информационной защиты объектов и компьютерных сетей. М.: ООО «Фирма «Издательство ACT»; СПб.: ООО «Издательство «Полигон», 2000. - 272 с. («Шпионские штучки»).

175. Соловьев А.Б. Доказывание в досудебных стадиях уголовного процесса России. Научно-практическое пособие. М.: ООО Издательство «Юрлитинформ», 2001. - 160 с.

176. Соловьев А.Б. Использование доказательств при допросе на предварительном следствии. Методическое пособие. М.: ООО Издательство «Юрлитинформ», 2001. - 136 с.

177. Соловьев А.Б. Как организовать расследование. Учебно-методическое пособие. М.: ООО Издательство «Юрлитинформ», 2000. - 88 с.

178. Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. Защита информации в персональных ЭВМ. М.: Радио и связь, МП «Веста», 1992. - 192 с.

179. Справочная книга криминалиста / Под ред. Н.А.Селиванова. М.: Издательство НОРМА (Издательская группа НОРМА-ИНФРА\*М), 2000. - 727 с.

180. Степанов Е.А. Управление персоналом: Персонал в системе защиты информации: Учебное пособие. М.: Форум: ИНФРА'М, 2002. -288 с.

181. Тайли Э. Безопасность персонального компьютера / Пер. с англ. -Мн.: ООО «Попурри», 1997. 480 с.

182. Теоретические основы компьютерной безопасности: Учебное пособие. / Девянин П.Н., Михальский О.О., Правиков Д.И. и др. М.: Радио и связь, 2000. - 192 с.

183. Теория и практика обеспечения информационной безопасности / Под ред. П.Д.Зегжды. М.: Издательство Агентства «Яхтсмен», 1996. - 192 с. - Серия «Защита информации» (книга вторая).

184. Терентьев A.M. Антивирусная защита ПК в Windows 95/98/NT: Справочное руководство по антивирусным средствам ЗАО «Диалог-Наука». М.: Перспектива, 2000. - 104 с.

185. Терминология в области защиты информации. Справочник. М.: ВНИИ стандарт, 1993. - 49 с.

186. Толеубекова Б.Х. Компьютерная преступность: вчера, сегодня, завтра. Караганда: Карагандинская ВШ Государственного следственного комитета Республики Казахстан, 1995. - 155 с.

187. Толеубекова Б.Х. Организационно-правовые проблемы контроля над компьютерной преступностью: Учебное пособие. Караганда: ВШ МВДРК, 1994.-68 с.

188. Торонин А.А. Основы инженерно-технической защиты информации. М.: «Ось-89», 1998. - 336 с.

189. Файтс Ф., Джонстон П., Кратц М. Компьютерный вирус: проблемы и прогноз: Пер. с англ. М.: Мир, 1994. - 176 с.

190. Фигурнов В.Э. IBM PC для пользователя. М.: ИНФРА'М, 1998. -640 с.

191. Фоменков Г.В., Азаркин А.В., Любезнов Л.Н., Ерхов Е.В. Методы и средства обеспечения безопасности в сети Интернет. Научно-практическое пособие. М.: Войсковая часть 33965, 1997. - 112 с.

192. Фролов А.В., Фролов Г.В. Глобальные сети компьютеров. Практическое введение в Internet, E-Mail, FTP, WWW и HTML, программирование для Windows Sockets. M.: ДИАЛОГ-МИФИ, 1996.288 с. - (Библиотека системного программиста; Т. 23).

193. Фролов А.В., Фролов Г.В. Осторожно: компьютерные вирусы. М.: ДИАЛОГ-МИФИ, 1996. - 256 с.

194. Фэри Д. Секреты супер-хакера. СПб: Издательский дом «Невский проспект», 1997. - 384 с.

195. Чурилов С.Н. Криминалистическая методика: История и современность. М.: Издательско-книготорговый центр «Маркетинг», 2002. -370 с.

196. Шаталов А.С. Криминалистические алгоритмы и программы. Теория. Проблемы. Прикладные аспекты. М.: Лига Разум, 2000. -252 с.

197. Шумилов А.Ю. Проблемы законодательного регулирования оперативно-розыскной деятельности в России: Монография. М.: Академия ФСБ РФ, 1997.-232 с.

198. Щербаков А.Ю. Защита от копирования. М.: Эдель, 1992. - 80 с.

199. Щербаков А.Ю. Разрушающие программные воздействия.- М.: Эдель, 1993.- 63 с.

200. Яблоков Н.П. Криминалистическая методика расследования. М.: Изд-во Московского университета, 1985. - 98 с.

201. Ярочкин В.И. Безопасность информационных систем.- М.: «Ось-89», 1996. 320 с. (Безопасность предпринимательства).

202. Ярочкин В.И. Информационная безопасность. Учебное пособие. -М.: Международные отношения, 2000. 400 с.

203. Ярочкин В.И. Технические каналы утечки информации. М.: ИП-КИР, 1994. - 106 с.

204. Ярочкин В.И., Шевцова Т.А. Словарь терминов и определений по безопасности и защите информации. М.: «Ось-89», 1996.- 48 с. (Безопасность предпринимательства).1. Статьи

205. Браун Д., Гундерсон Л., Эван М. Интерактивный анализ компьютерных преступлений. / Открытые системы, № 11, 2000. С.40-49.

206. Вир-ту-альность. / Хакер, № 1, январь 2000. С.64-66.

207. Внутренняя сетевая атака с целью компрометации начальника. / BYTE/Россия, № 7/8, 1999.

208. Воронов А., Кирюшкин С. Как определить «ахиллесову пяту» в обеспечении безопасности своей информационной системы. / BYTE/Россия, № 1, 2000.- С.66-71.

209. Востриков А. Еще раз о безопасности. / BYTE/Россия, № 8, 2000. -С.44-54.

210. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: развитие, итоги, перспективы. // Зарубежная радиоэлектроника, № 3, 1993. С.3-21.

211. Герасименко В.А. Комплексная защита информации в современных системах обмена данными // Зарубежная радиоэлектроника, № 2, 1993.-C.3-29.

212. Гудков П.Б. Компьютерная преступность: возникновение, современное состояние и тенденции // Конфидент, № 4, 1995. С. 17-25.

213. Кадлоф А. Вирусы. / Компьютер, № 1, 1990. С.44-47.

214. Как защититься от макровирусов и троянских коней в Word-документах, если Вы работаете в Word 97. / BYTE/Россия, № 6/7, 2000. 60 с.

215. Карасик И. Математические аспекты компьютерных вирусов. / Компьютер Пресс, 1992. № 10 - С.51-56, № 11 - С.59-69.

216. Карасик И.Ш. Анатомия и физиология вирусов. / Интеркомпьютер, № 1, 1991, С.39-47.

217. Карден Филип. Охота за вирусом: взять живым или мертвым. / Сети и системы связи, № 1, 1999. С. 108.

218. Карден Филип. Пограничный контроль: руководство по антивирусным шлюзам. / Сети и системы связи, № 8, 1999. С.97.

219. Карден Филип. Средства антивирусной защиты серверов. / Сети и системы связи, № 9, 1999. С.97.

220. Касперски Крис. Атака на Unix. / Открытые системы, № 9, 2000. -С.54-61.

221. Касперски Крис. Макровирусы «рога и копыта» конца XX века. / BYTE/Россия, № 11, 1999. - С.62-67.

222. Касперски Крис. Почему не срабатывают антивирусы ? / BYTE/Россия, № 7/8, 1999.

223. Касперский Е. Создать компьютер, защищенный от вирусов можно. Но заставить людей работать с ним нельзя. / Известия, 15.08.2001 г.

224. Касперский Е., Зенкин Д. Ареал обитания вирусов не ограничен компьютерами. / Коммерсантъ, № 92 (25 мая), 2000.

225. Компьютерные преступления. Правовая база для борьбы с ними. / Профессионал, № 3 (19), 1997. С.29-34.

226. Крылов В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации. / Уголовное право, № 3, июль-сентябрь, 1998.

227. Курушин В.Д., Шопин А.В. Предупреждение и раскрытие преступлений, совершаемых с использованием компьютерной техники // Криминалистика и компьютерная преступность. Материалы научно-практического семинара. М., 1993. С.4.

228. Кустов В., Федчук А., Тугарев А., Блудилин К. Стеганография. Сокрытие информации в звуковых файлах. / BYTE/Россия, № 10, 2000. С.32-39.

229. Кустов В.Н., Федчук А.А., Поспишенко А.В. Стеганография. Сокрытие информации в графических файлах. / BYTE/Россия, № 5, 2000. С.38-44.

230. Леннон Э. Компьютерные атаки: что это такое и как с этим бороться. / BYTE/Россия, № 2, 2000. С.51-54.

231. Лопатин В.Н. Правовая охрана и защита коммерческой тайны. // Законодательство, № 1, 1998. С.77-82.

232. Лукацкий А.В. Новые грани обнаружения и отражения угроз. / Системы безопасности, связи и телекоммуникаций, № 36, 2000.

233. Лукацкий А.В. Обман прерогатива не только хакеров. / BYTE/Россия, № 2, 2000. - С.46-49.

234. Лукацкий А.В. Сетевая безопасность переходит на аппаратный уровень. / BYTE/Россия, № 11, 2000. С.62-65.

235. Моисеенко И. Основы безопасности информационных систем. / Компьютер Пресс, №№ 10-12, 1991.

236. Моисеенко И. Основы безопасности информационных систем. / Компьютер Пресс, №№ 10-12, 1991.

237. Онтаньон Рамон Дж. Выгоды и опасности электронного обмена сообщениями. / LAN/Журнал сетевых решений, № 10, 2000. С.40-48.

238. Онтаньон Рамон Дж. Создание эффективной системы выявления атак. / LAN/Журнал сетевых решений, № 10, 2000. С.86-91.

239. Панишев А. Разум под прицелом: информационные технологии против психики. / Подводная лодка, № 6, 2000. С.38-48.

240. Поваляев Е. Информационная безопасность или Спасение утопающих дело рук самих утопающих. / Компьютер Пресс, № 7, 2000. -С.75-86.

241. Прохоров А. Антивирус как элемент комплексной системы безопасности. / Компьютер Пресс, № 7, 2000. С. 69-74.

242. Райан Филипп. Внутренние атаки. / LAN/Журнал сетевых решений, № 4, 2000. С.42-49.

243. Ричардсон Р. Корпоративное антивирусное программное обеспечение. / LAN/Журнал сетевых решений, № 4, 2000. С.42-49.

244. Сабо Курт. Программы компьютерного андеграунда. / Планета Интернет, № 42. С.48-49.

245. Сырков Б. Троянские программы. / Системы безопасности, связи и телекоммуникации, № 30, 1999. С.66-69.

246. Трояны. Классификация. / Хакер, № 1, январь 2000. С.62-64.

247. Туманов Г.А. Организация как функция государственного управления // Советское государство и право. 1986. № 1. - С.38-41.

248. Федоров А. Защита компьютеров от хищений. / Компьютер Пресс, №7, 2000.-С.З 8-39.

249. Федоров А. Программная защита компьютеров и файлов. / Компьютер Пресс, № 7, 2000. С.38-39.

250. Федоров В. Компьютерные преступления: выявление, расследование и профилактика. / Законность, № 6, 1994. С.44-47.

251. Черных А.В. Обеспечение безопасности автоматизированных информационных систем (уголовно-правовые аспекты) // Советское государство и право, № 6, 1990. С.118.

252. Черных Э., Черных А. Компьютерные хищения: как их предотвратить? // Юстиция, № 3, 1993. С.21-22.

253. Экономические преступления с помощью компьютера. / Телохранитель, № 4, 1996. С.32-36.

*Для* ззаказа доставки данной работы воспользуйтесь поиском на сайте по ссылке: <http://www.mydisser.com/search.html>