МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Физико-технический факультет**

**Кафедра теоретической физики и компьютерных технологий**

**КУРСОВОЙ ПРОЕКТ**

**МАТЕМАТИЧЕСКИЕ МЕТОДЫ АНАЛИЗА УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И МЕТОДЫ ИХ ВЕРИФИКАЦИИ**

Работу выполнил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Тимошенко Кирилл Вадимович

Курс 2

Направление 09.03.02 Информационные системы и технологии

Научный руководитель

преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Т.В.Арутюнян

Нормоконтролер инженер \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Г.Д.Цой

Краснодар 2018

**Реферат**

Курсовой проект 40 с., 2 рис., 10 источников.

ВЕРИФИКАЦИЯ, БЕЗОПАСНОСТЬ ИНФОРМАЦИИ, АНАЛИЗ УГРОЗ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ВИРУС, МАТЕМАТИЧЕСКИЕ МЕТОДЫ, ИНФОРМАЦИОННАЯ СИСТЕМА

Объектом разработки данного курсового проекта являются основные угрозы безопасности информации.

Цель работы заключается в исследовании методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

В результате выполнения курсового проекта я пришел к выводу, что использование высокоэффективных информационных систем является обязательным условием успешной деятельности современных организаций и предприятий.

**СОДЕРЖАНИЕ**

Обозначения и сокращения………………………………………………………3

Введение…………………………………………………………………………...4

1 Угрозы информационной безопасности

1.1 Основные угрозы безопасности информации…………………….…….5

1.2 Характеристика компьютерных вирусов и признаки вирусного заражения……………………………..……………………………….6

1.3 Классификация компьютерных вирусов………………………….……..9

1.4 Анализ угроз информационной безопасности………….……………...15

2 Профилактика угроз информационной безопасности

2.1 Способы реализации угроз информационной безопасности…………16

2.2 Процесс определения угрозы безопасности информации в информационной системе…………………………………………19

3 Математические методы анализа угроз безопасности

3.1 Понятие Марковского случайного процесса применительно к АИС…………………………………………………………............27

3.2Постановка задачи. Допущения. Граф состояния системы…………...27

3.3 Определение вероятностей перехода АИС в каждое возможное состояние …………………………………………………………...29

4 Методы верификации

4.1 Верификация на основе конечных автоматов…………………………35

4.2 Проверка модели (model-checking)……………………………….…….35

4.3 Метод проверки типа (type checking)…………………………….…….36

Заключение………………………………………………….……………….…...38

Список использованных источников………………….........…………………..39

**Обозначения и сокращения**

|  |  |
| --- | --- |
| БД | База данных |
| ПО | Программное обеспечение |
| КС | Компьютерная сеть |
| АС | Автоматизированная система |
| ИБ | Информационная безопасность |
| УБИ | Угроза безопасности информации |
| ВС | Вычислительная сеть |

**ВВЕДЕНИЕ**

Проблемы защиты информации от постороннего доступа и нежелательного воздействия возникло тогда, когда человеку по каким-либо причинам не хотелось делиться ею ни с кем или не с каждым человеком.

Ценной становится информация, обладание которой позволит её существующему и потенциальному владельцам получить какую-либо выгоду.

С переходом на использование технических средств связи, информация подвергается воздействию случайных процессов, которые могут привести к ее разрушению, изменению на ложную, а также создать предпосылки к доступу к ней посторонних лиц.

С появлением сложных автоматизированных систем управления, связанных с автоматизированным вводом, обработкой, хранением и выводом информации, проблемы ее защиты приобретают еще большее значение.

Объектом исследования данного курсового проекта являются основные угрозы безопасности информации.

Предмет информационной безопасности рассматривается по целям существования субъектов, на основании чего предмет исследования сводится в область управления активными системами и формируется понятие информационной безопасности.

Цель работы заключается в комплексной формулировке подхода к определению состояния (условий) информационной безопасности, которое можно рассматривать как целевое состояние политики ИБ.

**1 Угрозы информационной безопасности**

**1.1 Основные угрозы безопасности информации**

К основным угрозам безопасности информации и нормального функционирования ИС относятся:

- утечка конфиденциальной информации;

- компрометация информации;

- несанкционированное использование информационных ресурсов;

- ошибочное использование информационных ресурсов;

- несанкционированный обмен информацией между абонентами;

- отказ от информации;

- нарушение информационного обслуживания;

- незаконное использование привилегий.

Менеджерам следует помнить, что довольно большая часть причин и условий, создающих предпосылки и возможность неправомерного овладения конфиденциальной информацией, возникает из-за элементарных недоработок и ошибок руководителей организации и их сотрудников. В настоящее время борьба с информационными инфекциями представляет значительные трудности, так как помимо невнимательности руководителей существует и постоянно разрабатывается огромное множество вредоносных программ, цель которых – порча БД и ПО компьютеров. Большое число разновидностей этих программ не позволяет разработать постоянных и надежных средств защиты против них.

Вредоносные программы классифицируются следующим образом:

- логические бомбы;

- троянский конь;

- компьютерный вирус;

- червь;

- захватчик паролей.

Приведенная классификация наиболее опасных вредоносных программ безопасности ИС не охватывает всех возможных угроз этого типа. И так как существует огромное количество угроз, было бы целесообразнее остановить свое внимание на одном из самых распространенных видов вредоносных программ, как компьютерный вирус.

**1.2 Характеристика компьютерных вирусов и признаки вирусного заражения**

На сегодняшний день известно более 45000 вирусов, и их число продолжает увеличиваться. Источниками вирусной грозы является электронная почта, подавляющее большинство вирусов проникает с помощью посланий через e-mail. Следом за ней идет информация, которая скачивается с web-сайтов. Часть вирусов переносится накопителями информации.

По данным исследования компании Symantec, в первом полугодии 2005 г. зарегистрировано 11 тыс. новых модификаций вирусов. Количество угроз, с которыми сталкиваются пользователи, возрастает с каждым годом, а сами вредоносные программы становятся все более и более сложными. Связано это с тем, что хакерский бизнес приносит большие прибыли. Время между обнаружением уязвимости компьютеров до выпуска соответствующей защиты в среднем составляет около одного-двух месяцев. Все это время компьютер практически беззащитен. Разрабатываются все более изощренные, трудноуловимые программы, которые научились отключать антивирусную защиту, сетевые экраны и прочие меры обеспечения безопасности. Большое распространение получают модульные, вредоносные программы, которые после заражения системы загружают дополнительные модули с расширенной функциональностью. Тогда они могут делать с компьютером пользователя все, что угодно, например, рассылать с него спам, т.е. осуществлять рассылку нежелательных электронных писем. Среди новых угроз называется установка рекламного ПО «adware» и «фишинг». «Adware» открывает окна и отображает рекламные сообщения на web-сайтах. А «фишингом» эксперты называют попытки получить конфиденциальные, в основном, финансовые сведения, например, номер и пин-код кредитных карт.

Компьютерный вирус — это небольшая по размерам программа, которая заражает другие программы, например, приписывая себя к ним, и выполняет различные, вредоносные действия на компьютере — портит, удаляет файлы или таблицу размещения файлов на диске, засоряет оперативную память, рассылает себя по Интернету и т.д. Когда такая программа начинает исполняться, то сначала управление получает вирус, который находит и заражает другие программы. Вирус маскируется в системе. Например, после того как вирус выполнит вредоносные действия, он передает управление той программе, в которой находится, и она работает обычным образом. Таким образом, работа зараженного компьютера внешне выглядит так же, как и незараженного. Вред вируса проявится позднее, когда, возможно, уже поздно спасать как информацию, так и сам компьютер. Компьютерный вирус может испортить любой файл, вызвав потерю информации на жестких дисках компьютера. Вначале они могут незаметно заразить большое число программ и дисков, а затем вызвать серьезные повреждения, например отформатировав весь жесткий диск на компьютере.

Вирус – это программа, обладающая способностью к самостоятельному внедрению в компьютерный код других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но и могут вообще с ним не совпадать. Вирус не может существовать в «полной изоляции»: нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна — вирус должен каким-нибудь способом обеспечить передачу себе управления. Вирус, в основном, внедряется в рабочую программу так, чтобы при ее запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус, прежде всего, переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, становится возможным заражение других файлов.

Предшественниками вирусов принято считать так называемые троянские программы (программа, используемая злоумышленником для сбора информации, ее разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях), тела которых содержат скрытые последовательности команд (модули), выполняющие действия, наносящие вред пользователям. Наиболее распространенной разновидностью троянских программ являются широко известные программы массового применения (редакторы, игры, трансляторы и т.д.), в которые встроены так называемые «логические бомбы» (программа для искажения или стирания информации) , срабатывающие по наступлении некоторого события. Известно, что троянские программы не являются саморазмножающимися.

Принципиальное отличие вируса от троянской программы состоит в том, что вирус после его активизации существует автономно и в процессе своего функционирования инфицирует программы путем включения в них своего текста. Таким образом, компьютерный вирус можно рассматривать как своеобразный «генератор троянских программ». Программы, зараженные вирусом, называют “вирусоносителями”.

Наиболее часто заражаются загрузочный сектор диска и исполняемые файлы, с расширениями .EXE, .COM, .SYS, .ВАТ. Редко заражаются текстовые файлы.

После заражения программы вирус может выполнить какую-нибудь диверсию, не слишком серьезную, чтобы не привлечь внимания. И наконец, не забывает возвратить управление той программе, из которой он был воспроизведён. Каждое выполнение зараженной программы переносит вирус в последующую. Таким образом, заражается практически всё программное обеспечение.

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним относятся:

- прекращение работы или некорректная работа ранее успешно функционировавших программ;

- замедление работы компьютера;

- невозможность загрузки операционной системы;

- исчезновение файлов и каталогов или изменение их содержимого;

- изменение даты и времени модификации файлов;

- изменение объёмов файлов;

- неожиданное значительное увеличение количества файлов на диске;

- существенное уменьшение размера свободной оперативной памяти;

- вывод на экран непредусмотренных сообщений или изображений;

- подача непредусмотренных звуковых сигналов;

- частые зависания и сбои в работе компьютера.

Следует понимать, что вышеперечисленные явления не всегда вызываются присутствием вируса, а могут быть следствием других причин. И это затрудняет правильную диагностику состояния компьютера.

Итак, если не предпринимать мер по защите от вирусов, то последствия заражения компьютера могут быть весьма серьезными.

**1.3 Классификация компьютерных вирусов**

Заражение программы, как правило, выполняется таким образом, чтобы вирус получил управление раньше самой программы. Для этого он либо встраивается в начало программного кода, либо в ее тело так, что первой командой зараженной программы является безусловный переход на компьютерный вирус, текст которого заканчивается аналогичной командой безусловного перехода на команду вирусоносителя, бывшую первой до заражения. Получив управление, вирус выбирает следующий файл, заражает его, возможно, выполняет какие-либо другие действия, после чего отдает управление вирусоносителю.

«Первичное заражение происходит в процессе наступления инфицированных программ из памяти одной машины в память другой, причем в качестве средства перемещения этих программ могут использоваться как носители информации (оптические диски, флэш-память и т.п.), так и каналы вычислительных сетей. Вирусы, использующие для размножения сетевые средства, сетевые протоколы, управляющие команды компьютерных сетей и электронной почты, принято называть сетевыми.

Цикл жизни вируса обычно включает следующие периоды: внедрение, инкубационный, репликации (саморазмножения) и проявления. В течение инкубационного периода вирус неактивен, что усложняет задачу его поиска и нейтрализации. На этапе проявления вирус выполняет свойственные ему целевые функции, например необратимую коррекцию информации в компьютере или на носителях.

Физическая структура компьютерного вируса достаточно проста. Он состоит из головы и, возможно, хвоста. Под головой вируса понимается его компонент, получающий управление первым. Хвост – это часть вируса, расположенная в тексте зараженной программы отдельно от головы. Вирусы, состоящие из одной головы, называют несегментированными, тогда как вирусы, содержащие голову и хвост, - сегментированными.

Наиболее существенные признаки компьютерных вирусов позволяют провести следующую их классификацию (рисунок 1).

|  |
| --- |
|  |



Рисунок 1 - Классификация вирусов

По режиму функционирования:

- резидентные вирусы (вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к ресурсам);

- транзитные вирусы (вирусы, которые выполняются только в момент запуска зараженной программы).

По объекту внедрения:

- файловые вирусы (вирусы, заражающие файлы с программами);

- загрузочные вирусы (вирусы, заражающие программы, хранящиеся в системных областях дисков).

В свою очередь, файловые вирусы подразделяются на вирусы, заражающие:

- исполняемые файлы;

- командные файлы и файлы конфигурации;

- составляемые на макроязыках программирования, или файлы, содержащие макросы (макровирусы -разновидность компьютерных вирусов разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office);

- файлы с драйверами различных устройств;

- файлы с библиотеками исходных, объектных, загрузочных и оверлейных модулей, библиотеками динамической компоновки и т.п.

Загрузочные вирусы подразделяются на вирусы, заражающие:

- системный загрузчик, расположенный в загрузочном секторе и логических дисков;

- внесистемный загрузчик, расположенный в загрузочном секторе жестких дисков.

По степени и способу маскировки:

- вирусы, не использующие средств маскировки;

- stealth-вирусы (вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных);

- вирусы-мутанты (MtE-вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса).

В свою очередь, последние делятся:

- на обычные вирусы-мутанты, в разных копиях которых различаются только зашифрованные тела, а дешифрованные тела вирусов совпадают;

- полиморфные вирусы, в разных копиях которых различаются не только зашифрованные тела, но и их дешифрованные тела.

Наиболее распространенные типы вирусов характеризуются следующими основными особенностями.

Файловый транзитный вирус целиком размещается в исполняемом файле, в связи с чем он активизируется только в случае активизации вирусоносителя, а по окончании выполнения необходимых действий возвращает управление самой программе. При этом выбор очередного файла для заражения осуществляется вирусом посредством поиска по каталогу.

Файловый резидентный вирус отличается от нерезидентного логической структурой и общим алгоритмом функционирования. Резидентный вирус состоит из так называемого инсталлятора и программ обработки прерываний. Инсталлятор получает управление при активизации вирусоносителя и инфицирует оперативную память путем размещения в ней управляющей части вируса и замены адресов в элементах вектора прерываний на адреса своих программ, обрабатывающих эти прерывания. На так называемой фазе слежения, следующей за описанной фазой инсталляции, при возникновении какого-либо прерывания управление получает соответствующая подпрограмма вируса. В связи с существенно более универсальной по сравнению с нерезидентными вирусами общей схемой функционирования резидентные вирусы могут реализовывать самые разные способы инфицирования.

Наиболее распространенными способами являются инфицирование запускаемых программ, а также файлов при их открытии или чтении. Отличительной особенностью последних является заражение загрузочного сектора магнитного носителя. Голова загрузочного вируса всегда находится в загрузочном секторе (единственном для гибких дисков и одном из двух – для жестких), а хвост – в любой другой области носителя. Наиболее безопасным для вируса способом считается размещение хвоста в так называемых псевдосбойных кластерах, логически исключенных из числа доступных для использования. Существенно, что хвост загрузочного вируса всегда содержит копию оригинального (исходного) загрузочного сектора.

Stealth -вирусы пользуются слабой защищенностью некоторых операционных систем и заменяют некоторые их компоненты (драйверы дисков, прерывания) таким образом, что вирус становится невидимым (прозрачным) для других программ.

Полиморфные вирусы содержат алгоритм порождения дешифрованных тел вирусов, непохожих друг на друга. При этом в алгоритмах дешифрования могут встречаться обращения практически ко всем командам процессора Intel и даже использоваться некоторые специфические особенности его реального режима функционирования.

Макровирусы распространяются под управлением прикладных программ, что делает их независимыми от операционной системы. Подавляющее число макровирусов функционирует под управлением текстового процессора Microsoft Word. В то же время известны макровирусы, работающие под управлением таких приложений, как Microsoft xcel, Lotus Ami Pro, Lotus 1-2-3, Lotus Notes, в операционных системах фирм Microsoft и Apple.

Сетевые вирусы, называемые также автономными репликативными программами, или, для краткости, репликаторами, используют для размножения средства сетевых операционных систем. Наиболее просто реализуется размножение в тех случаях, когда сетевыми протоколами возможно и в тех случаях, когда указанные протоколы ориентированы только на обмен сообщениями. Классическим примером реализации процесса электронной почты является репликатор Морриса. Текст репликатора передается от одной ЭВМ к другой как обычное сообщение, постепенно заполняющее буфер, выделенный в оперативной памяти ЭВМ-адресата. В результате переполнения буфера, инициированного передачей, адрес возврата в программу, вызвавшую программу приема сообщения, замещается на адрес самого буфера, где к моменту возврата уже находится текст вируса.

Тем самым вирус получает управление и начинает функционировать на ЭВМ-адресате.

«Лазейки», подобные описанной выше обусловленные особенностями реализации тех или иных функций в программном обеспечении, являются объективной предпосылкой для создания и внедрения репликаторов злоумышленниками. Эффекты, вызываемые вирусами в процессе реализации ими целевых функций, принято делить на следующие группы:

- искажение информации в файлах либо в таблице размещения файлов (FAT-таблице), которое может привести к разрушению файловой системы в целом;

- имитация сбоев аппаратных средств;

- создание звуковых и визуальных эффектов, включая, например, отображение сообщений, вводящих оператора в заблуждение или затрудняющих его работу;

- инициирование ошибок в программах пользователей или операционной системе.

**1.4 Анализ угроз информационной безопасности**

Для успешного противодействия угрозам и атакам КС, а так же выбора способов и средств защиты, политики безопасности и анализа рисков от возможности несанкционированного доступа необходимо классифицировать существующие угрозы информационной безопасности. Каждый признак классификации должен отражать одно из обобщенных требований к системе защиты, а сами угрозы позволяют детализировать эти требования. Современные КС и сети являются сложными системами, подверженными так же влиянию очень большого числа факторов, и поэтому формализовать задачу описания полного множества угроз не представляется возможным. Как следствие, для защищенной КС определяется не полный перечень угроз, а перечень классов угроз, которым должен противодействовать комплекс средств защиты.

**2 Профилактика угроз информационной безопасности**

**2.1 Угрозы информационной безопасности и способы их реализации**

Выявление и анализ возможных угроз информационной безопасности проводится с целью определения полного перечня требований к разрабатываемой системе защиты. Под угрозой информационной безопасности АС понимается возможность реализации воздействия на информацию, обрабатываемую в АС, приводящего к искажению уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носители информации, средства взаимодействия с носителем или средства его управления.

В соответствии с существующими подходами принято считать, что информационная безопасность АС обеспечена в случае, если для любых информационных ресурсов в системе поддерживается определённый уровень конфиденциальности (невозможности несанкционированного получения какой-либо информации), целостности (невозможности несанкционированной или случайной её модификации) и доступности (возможности за разумное время получить требуемую информацию). Соответственно для АС имеет смысл рассматривать три основных вида угроз.

а) угроза нарушения конфиденциальности. Заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой («утечка»);

б) угроза нарушения целостности. Любое умышленное изменение информации, хранящейся в ВС или передаваемой от одной системы в другую;

в) угроза отказа служб. Возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу АС. Реально блокирование может быть постоянным (запрашиваемый ресурс никогда не будет получен) или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным (ресурс исчерпан).

Данные виды угроз можно считать первичными или непосредственными, так как если рассматривать понятие угрозы как некоторой потенциальной опасности, реализация которой наносит ущерб информационной системе, то реализация вышеперечисленных угроз приведёт к непосредственному воздействию на защищаемую информацию. В то же время непосредственное воздействие на информацию возможно для атакующей стороны в том случае, если система, в которой циркулирует информация, для неё «прозрачна», т.е. не существует никаких систем защиты или других препятствий.

На современном этапе развития информационных технологий подсистемы или функции защиты являются неотъемлемой частью комплексов по обработке информации. Информация не представляется в чистом виде. На пути к ней имеется хотя бы какая-нибудь система защиты, которую необходимо преодолеть атакующей стороне. Однако не существует абсолютно стойкой системы защиты, вопрос лишь во времени и средствах, требующихся на её преодоление.

Исходя из данных условий приемлемой можно считать следующую модель: защита информационной системы считается преодолённой, если в ходе её исследования определены все уязвимости системы. Поскольку преодоление защиты также представляет собой угрозу, то для защищённых систем рассматривается четвёртый вид угроз – угроза раскрытия параметров АС, включающей в себя систему защиты.

Угрозу раскрытия можно считать опосредствованной, поскольку последствия её реализации не причиняют вред обрабатываемой информации, но дают возможность реализовываться непосредственным угрозам.

Отличие защищённых информационных систем от открытых заключается в том, что для последних угроза раскрытия параметров системы считается реализованной.

В настоящее время рассматривается достаточно обширный перечень угроз информационной безопасности АС, которые могут быть классифицированы по ряду признаков:

- по природе возникновения (естественные или искусственные);

- по степени преднамеренности проявления (случайного действия или преднамеренного);

- по непосредственному источнику (природная среда, человек, санкционированные программные средства и несанкционированные программные средства);

- по положению угроз (источник угроз вне контролируемой зоны, в пределах контролируемой зоны, источник имеет доступ к периферийным устройствам и источник которых расположен в АС);

- по степени зависимости от активности АС (проявляющиеся независимо от активности АС и проявляющиеся только в процессе автоматизированной обработки данных);

- по степени воздействия на АС (пассивные и активные)

- по этапам доступа пользователей или программ к ресурсам АС (проявляющиеся на этапе доступа к ресурсам и проявляющиеся после разрешения доступа к ресурсам);

- по способу доступа к ресурсам АС (направленные на использование прямого стандартного пути доступа к ресурсам и направленные на использование скрытого нестандартного доступа к ресурсам АС) ;

- по текущему месту расположения информации, хранимой и обрабатываемой в АС (угрозы доступа к информации на внешнем запоминающем устройстве; угрозы доступа к информации в оперативной памяти; угрозы доступа к информации, циркулирующей в линиях связи; угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере).

**2.2 Процесс определения угрозы безопасности информации в информационной системе**

Целью определения угроз безопасности информации является установление того, существует ли возможность нарушения конфиденциальности, целостности или доступности информации, содержащейся в информационной системе, и приведет ли это нарушение хотя бы одного из указанных свойств безопасности информации к наступлению неприемлемых негативных последствий для обладателя информации или оператора, а в случае обработки персональных данных и для субъектов персональных данных.

Определение угроз безопасности информации должно носить систематический характер и осуществляться как на этапе создания информационной системы и формирования требований по ее защите, так и в ходе эксплуатации информационной системы. Систематический подход к определению угроз безопасности информации необходим для того, чтобы определить потребности в конкретных требованиях к защите информации и создать адекватную эффективную систему защиты информации в информационной системе. Меры защиты информации, принимаемые обладателем информации и оператором, должны обеспечивать эффективное и своевременное выявление и блокирование (нейтрализацию) угроз безопасности информации, в результате реализации которых возможно наступление неприемлемых негативных последствий (ущерба).

Систематический подход к определению угроз безопасности информации предусматривает реализацию непрерывного процесса, в рамках которого определяется область применения процесса определения угроз, идентифицируются источники угроз и угрозы безопасности информации, оценивается возможность реализации угроз безопасности информации и степень возможного ущерба в случае такой реализации, осуществляется мониторинг (периодический пересмотр) и переоценка угроз безопасности информации.

Оценка угроз безопасности информации проводится экспертным методом.

Область применения процесса определения угроз безопасности информации. На этапах принятия решения о необходимости защиты информации в информационной системе и разработки требований к защите информации должны быть определены физические и логические границы информационной системы, в которых принимаются и контролируются меры защиты информации, за которые ответственен оператор, а также определены объекты защиты и сегменты информационной системы.

Процесс определения угроз безопасности информации должен охватывать все объекты защиты и сегменты в логических и физических границах информационной системы, в которых оператором принимаются и контролируются меры защиты информации. Процесс определения угроз безопасности информации организуется подразделением оператора, назначенным ответственным за защиту информации в информационной системе. В случае, если информационная система имеет сегменты, эксплуатируемые разными подразделениями оператора, которые могут самостоятельно принимать и контролировать меры защиты информации, должны быть определены границы ответственности этих подразделений и порядок их взаимодействия в процессе определения угроз безопасности информации.

Область применения процесса определения угроз безопасности информации отражается в модели угроз безопасности информации наряду с областью действия модели угроз, структурно-функциональными характеристиками информационной системы и особенностями ее функционирования.

- Идентификация источников угроз и угроз безопасности информации. В обобщенном виде угрозы безопасности информации характеризуется источниками угроз, факторами, обуславливающими возможность реализации угроз, способами (методами) реализации угроз и последствиями от реализации угроз безопасности информации.

Важным этапом в процессе определения угроз безопасности информации является идентификация лиц или событий (явлений), в результате действий (наступления, возникновения) которых возможно нарушение конфиденциальности, целостности или доступности информации, содержащейся в информационной системе, и возникновение неприемлемых негативных последствий (ущерба).

В качестве источников угроз безопасности информации могут выступать субъекты (физические лица, организации, государства) или явления (техногенные аварии, стихийные бедствия, иные природные явления).

Источники угроз безопасности информации являются определяющим фактором при определении угроз безопасности информации в информационных системах. В процессе определения угроз безопасности информации подлежат оценке те угрозы, у которых есть источники и источники имеют возможности и условия для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями ее функционирования.

Источники угроз безопасности информации могут быть следующих типов:

- антропогенные источники (антропогенные угрозы);

- техногенные источники (техногенные угрозы);

- стихийные источники (угрозы стихийных бедствий, иных природных явлений).

В качестве источников антропогенных угроз безопасности информации могут выступать:

- лица, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в информационной системе, или нарушения функционирования информационной системы или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности информации);

- лица, имеющие доступ к информационной системе, не преднамеренные действия которых могут привести к нарушению безопасности информации (непреднамеренные угрозы безопасности информации).

Для информационных систем, в которых целью защиты является обеспечение целостности и доступности обрабатываемой информации, в обязательном порядке подлежат оценке техногенные угрозы, связанные с отказами или сбоями в работе технических средств или программного обеспечения. Такие угрозы могут быть обусловлены:

- низким качеством (надежностью) технических, программных или программно-технических средств;

- низким качеством (надежностью) сетей связи и (или) услуг связи;

- отсутствием или низкой эффективностью систем резервирования или дублирования программно-технических и технических средств;

- низким качеством (надежностью) инженерных систем (кондиционирования, электроснабжения, охранных систем и т.д.);

низким качеством обслуживания со стороны обслуживающих организаций и лиц.

При определении угроз безопасности информации оценке подлежат угрозы, связанные со всеми типами источников. Однако в целях создания и эксплуатации адекватной эффективной системы защиты информации в информационной системе следует, в первую очередь, уделять внимание оценке антропогенных угроз, связанных с несанкционированными (неправомерными) действиями субъектов по нарушению безопасности (конфиденциальности, целостности, доступности) информации, в том числе целенаправленными воздействиями программными (программно-техническими) средствами на информационные системы, осуществляемые в целях нарушения (прекращения) их функционирования (компьютерные атаки).

Также при определении угроз безопасности информации наряду с угрозами, реализация которых может привести непосредственно к нарушению конфиденциальности, целостности или доступности информации (прямыми угрозами), необходимо выявлять и оценивать угрозы, создающие условия для реализации прямых угроз безопасности информации (косвенные угрозы). В качестве косвенных угроз безопасности информации могут рассматриваться угрозы повышения привилегий, исчерпания вычислительных ресурсов, недоступности обновления программного обеспечения и иные угрозы безопасности информации.

В процессе определения угроз безопасности информации на всех стадиях (этапах) жизненного цикла информационных систем необходимо регулярно проводить идентификацию источников угроз, оценивать их возможности и определять на этой основе угрозы безопасности информации. Данные о нарушителях и их возможностях по реализации угроз безопасности информации, полученные при идентификации источников угроз, включаются в модели угроз безопасности информации.

Для идентификации угроз безопасности информации в информационной системе определяются:

- возможности (тип, вид, потенциал) нарушителей, необходимые им для реализации угроз безопасности информации;

- уязвимости, которые могут использоваться при реализации угроз безопасности информации (включая специально внедренные программные закладки);

- способы (методы) реализации угроз безопасности информации;

- объекты информационной системы, на которые направлена угроза безопасности информации (объекты воздействия);

- результат и последствия от реализации угроз безопасности информации.

Каждая угроза безопасности информации в информационной системе описывается (идентифицируется) следующим образом: УБИi = [нарушитель (источник угрозы); уязвимости; способы реализации угрозы; объекты воздействия; последствия от реализации угрозы].

Оценка вероятности (возможности) реализации угроз безопасности информации и степени возможного ущерба. Идентифицированная угроза безопасности информации подлежит нейтрализации (блокированию), если она является актуальной (УБИi А ) для информационной системы, то есть в информационной системе с заданными структурно функциональными характеристиками и особенностями функционирования существует вероятность (возможность) реализации рассматриваемой угрозы нарушителем с соответствующим потенциалом и ее реализация приведет к неприемлемым негативным последствиям (ущербу): УБИi А = [вероятность (возможность) реализации угрозы (Рi); степень ущерба (Xi)].

Актуальные угрозы безопасности информации включаются в модель угроз безопасности информации. Модель угроз безопасности информации, учитывая особенности информационной системы, используемые в ней программные, программно-технические, технические средства и процессы обработки информации, дает описание угроз безопасности, которым подвержена информационная система.

Мониторинг и переоценка угроз безопасности информации. Определение угроз безопасности информации на этапе создания информационной системы позволяет обеспечить формирование требований и внедрение эффективной адекватной системы защиты информации в информационной системе для угроз, актуальных к моменту ввода в эксплуатацию информационной системы.

В ходе эксплуатации информационной системы оператор, обеспечивая достижение целей и задач информационной системы, может изменять ее базовую конфигурацию, что приводит к изменению структурно-функциональных характеристик информационной системы и применяемых информационных технологий. Также в процессе эксплуатации возможно изменение состава и значимости обрабатываемой информации и особенностей функционирования информационной системы.

В этих условиях процесс определения угроз безопасности информации должен носить систематический характер. В ходе эксплуатации информационной системы регулярно проводится анализ изменения угроз безопасности информации, а актуальные угрозы безопасности информации подлежат периодической переоценке. Периодичность переоценки определяется организацией исходя из особенностей функционирования информационной системы. Рекомендуется пересматривать угрозы безопасности информации не реже одного раза в год. По результатам анализа проводится уточнение (при необходимости) модели угроз безопасности информации.

Пересмотр (переоценка) угроз безопасности информации, как минимум, осуществляется в случаях:

- изменения требований законодательства Российской Федерации о защите информации, нормативных правовых актов и методических документов, регламентирующих защиту информации;

- изменения конфигурации (состава основных компонентов) и особенностей функционирования информационной системы, следствием которых стало возникновение новых угроз безопасности информации;

- выявления уязвимостей, приводящих к возникновению новых угроз безопасности информации или к повышению возможности реализации существующих;

- появления сведений и фактов о новых возможностях нарушителей.

**3 Математические методы анализа угроз безопасности**

**3.1 Понятие Марковского случайного процесса применительно к АИС**

Пусть на АИС в произвольный момент времени ti воздействует i-я угроза. В результате такого воздействия АИС переходит из состояния S0 в состояние Si .

Пусть в момент времени t < t0 АИС находилась в стационарном состоянии предшествующем воздействию i-й угрозы. Такое состояние характеризует предысторию процесса – прошлое состояние АИС до момента времени t0. В момент времени t0 на АИС воздействует i-я угроза, в результате которой АИС за время t1= t0+τ переходит из состояния S0 – о в состояние S1 – е. Если такой процесс соответствует Марковскому случайному процессу, то можно предсказать такой переход, учитывая только настоящее состояние АИС – S0 и, забыв о ее предыстории. Само состояние S0 зависит от прошлого, но, как только оно достигнуто, о прошлом состоянии можно забыть.

Таким образом, в Марковском случайном процессе будущее состояние АИС зависит от прошлого только через настоящее.

Итак, случайный процесс применительно к АИС называется Марковским, если для любого момента времени t0 вероятностные характеристики АИС в будущем зависят только от её состояния в данный момент t0 и не зависят от того, когда и как АИС пришла в это состояние.

**3.2 Постановка задачи. Допущения. Граф состояния системы**

Пусть на АИС за конечное время τ воздействует n простейших потоков угроз с интенсивностями λi , i =1,n [5–8, 11, 16].

Пусть μi – интенсивность парирования последствий i-й угрозы. Соответственно, Ri – вероятность парирования, а Ri – вероятность не парирования i-й угрозы.

Тогда, μi\*Ri ⋅ – интенсивность парирования, а μi\*Ri ⋅ – интенсивность не парирования последствий воздействия на АИС потока угроз.

Допущения:

- поток парирования и не парирования угрозы простейший;

- возможности по парированию последствий воздействия на АИС i-й угрозы не ограничены, т.е. μi ≥ λi ;

- так как рассматриваются простейшие потоки, то появление одновременно двух и более угроз является невозможным событием.

Для определения вероятности благополучного исхода при воздействии на АИС потока n угроз представим систему АИС в виде графа (рисунок 2).

В соответствии с рисунком 2 можно составить матрицу интенсивностей перехода вида.



Рисунок 2 - Граф состояний АИС



 (1)

где λ = λ + λ +… + λn;

 j = k =1,2,...,n + 2.

В соответствии с рисунок 2 АИС в момент времени τ может находиться в одном из следующих состояний:

- состояние «0» – поток угроз за время τ не проявился;

- состояние «1», …, i , …, n – одна из угроз проявилась;

- состояние « n +1 » – неблагополучное поглощающее состояние, при котором угроза реализовалась.

Матрица обладает следующими свойствами: диагональные члены матрицы равны сумме остальных элементов данной строки, взятых с обратным знаком; сумма всех элементов каждой строки равна нулю; число нулевых строк в матрице интенсивностей переходов соответствует количеству поглощающих состояний; интенсивность перехода равна нулю при отсутствии стрелки.

**3.3 Определение вероятностей перехода АИС в каждое возможное состояние**

Для определения вероятностей перехода АИС в каждое возможное состояние воспользуемся системой дифференциальных уравнений Колмогорова, в соответствии с которыми можно написать:

 (2)

.

Применяя к системе дифференциальных уравнений прямое преобразование Лапласа с учетом исходных данных P0 (0) =1, Pi(0) = Pn+1(0) = 0 и с учетом того, что , получим следующие выражения для определения вероятностей в соответствии с графом состояний (рисунок 2)

 (3)

где – искомое изображение.

При начальных условиях система уравнений примет вид:

 (4)

По правилу Крамера искомые изображения определяются отношением:

 (5)

где – главный определитель системы;

 Δj(S) – частный определитель системы, находится из главного определителя путем замены j-го столбца коэффициентами, стоящими в правых частях уравнений.

Частные определители, полученные с помощью введения определителей по индукции, будут равны:

 (6)

С учетом указанного и при условии, что , система уравнений примет вид:

 (7)

Окончательно с учетом выражения примут вид:

 (8)

Тогда следует, что вероятность благополучного исхода от воздействия на АИС n независимых потоков внутренних угроз определяется следующим выражением: а вероятность противоположного события, т.е. неблагополучного исхода, будет равна

Частный случай:

- Интенсивность парирования i-го потока угрозы μi равно интенсивности воздействия i-го потока угрозы λi

Пусть μi = λi , т.е. интенсивность парирования последствий i-го потока угроз равна интенсивности i-го потока угроз.

Тогда изображения вероятностей можно представить следующим образом:

 ;

 (9)

.

Функции qi(S) и ρ(S) могут быть представлены в виде полиномов с коэффициентами bi и ci , а именно:

 (10)

Из выражения следует, что изображения вероятностей Pj (S) являются правильными рациональными дробями, у которых степени полиномов числителей численно меньше полиномов знаменателей.

Тогда применяя табличное преобразование Лапласа, получим следующее выражение для характеристических оригиналов искомых вероятностей:

 (11)

где ω – количество корней i-го характеристического уравнения;

Тогда с учетом нормированного условия где Pi – вероятность нахождения АИС в i-м состоянии, можно записать, что конечная вероятность

 (12)

характеризует благополучный и неблагополучный исход.

 (13)

**4 Методы верификации**

**4.1 Верификация на основе конечных автоматов**

Конечные автоматы могут быть использованы не только для спецификации, но также и для проведения анализа криптографических протоколов. В этом случае применяется методика, известная под названием методика анализа достижимости.

Эта методика предполагает описание системы в следующем виде. Для каждого перехода строится глобальное состояние системы, которое выражается через состояния сущностей системы и состояния коммуникационных каналов между ними. Каждое глобальное состояние затем анализируется, и определяются его свойства, такие как тупик и корректность. Если сущность не способна получить сообщение, а предполагалось, что оно должно было быть получено в этом состоянии, тогда существует проблема в протоколе.

Методика анализа достижимости эффективна для определения корректности протокола по отношению к его спецификациям, однако она не гарантирует безопасности от активного злоумышленника.

**4.2Проверка модели (model-checking)**

Метод проверки модели впервые был предложен в начале 80-ых. В последнее время он становится индустриальной практикой и широко используется в практических приложениях, в особенности для проверки аппаратуры и коммуникационных протоколов, для анализа гибридных систем.

Метод заключается в специфицировании свойств системы на языке алгебры процессов или в виде формул темпоральной логики, построении модели в виде конечного автомата, автоматической проверке того, что эта модель удовлетворяет спецификации, причем при отрицательном выводе вырабатывается контрпример. Метод проверки модели состоит в переборе всех возможных переходов автомата из одного состояния в другое из некоего начального состояния системы. Все возможные трассы из начального набора состояний перебираются, чтобы убедиться в том, что все они являются безопасными, или доказать, что живучесть системы не может быть нарушена.

Метод проверки модели страдает недостатком, широко известным под названием “взрыв количества состояний“. При моделировании времени как непрерывной сущности даже самая простая модель имеет бесконечное число состояний. Наиболее известным подходом к решению этой проблемы является метод символической проверки модели, в котором проблема упрощается с помощью формирования классов эквивалентности. При этом используются компактные булевские формы для представления наборов состояний и переходов, как, например, BDDs (Binary Decision Diagrams), и накладываются некоторые ограничения на структуру пространства состояний.

**4.3 Метод проверки типа (type checking)**

Самым новым подходом к формальному анализу протоколов является использование метода проверки типа (type checking), введенным Абади (Abadi). Абади ввел тип untrusted (Un) для открытых сообщений, которые исходят от оппонента (в качестве оппонентов выступают все, кроме удостоверяющих принципалов).

В методе проверки типа сообщениям и каналам присваиваются типы (например, единица данных приватного типа появляется на открытом канале). Метод проверки типа имеет существенное достоинство, состоящее в том, что он, как и метод проверки модели, является полностью автоматическим, но в отличие от последнего способен оперировать с несколькими классами бесконечных систем. Однако он имеет потенциальный недостаток, состоящий в том, что, так как нарушения безопасности определены в терминах несогласованностей типа, требования безопасности, которые должны быть 53 доказаны, должны быть сформулированы в спецификации в процессе её написания. Это отличает метод проверки типов от метода проверки модели, для которого любое свойство безопасности, которое может быть выражено в терминах темпоральной логики, может специфицироваться независимо, уже после того, как сам протокол специфицирован.

**ЗАКЛЮЧЕНИЕ**

Статистика показывает, что во всех странах убытки от злонамеренных действий непрерывно возрастают. Причем основные причины убытков связаны не столько с недостаточностью средств безопасности как таковых, сколько с отсутствием взаимосвязи между ними, т.е. с нереализованностью системного подхода. Поэтому необходимо опережающими темпами совершенствовать комплексные средства защиты. Одной из основных задач защиты информации является организация эффективной антивирусной защиты автономных рабочих станций, локальных и корпоративных компьютерных сетей, обрабатывающих информацию ограниченного доступа, в том числе содержащую государственную и служебную тайну.

Из рассмотренного становится очевидно, что обеспечение информационной безопасности является комплексной задачей. Это обусловлено тем, что информационная среда является сложным многоплановым механизмом, в котором действуют такие компоненты, как электронное оборудование, программное обеспечение, персонал.

В ходе данной работы я освоил, что для решения проблемы обеспечения информационной безопасности необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

Также я пришел к выводу, что использование высокоэффективных информационных систем является обязательным условием успешной деятельности современных организаций и предприятий. Безопасность информации — это один из основных показателей качества информационной системы.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1 Саак А.Э. - Информационные технологии управления 2-е издание: Учебник для ВУЗов/ А.Э. Саак, Е.В. Пахомов, В.Н. Тюшняков – СПб.: Питер, 2009. – 407 с.

2 Информатика и информационные технологии: учебное пособие/ Ю. Д. Романова, И. Г. Лесничая, В. И. Шестаков, И. В. Миссинг, П. А. Музычкин. – М.: Эксмо, 2008. – 592 с.

3 Титоренко Г.А. Информационные технологии управления: Учеб. Пособие для ВУЗов/ Под ред. Проф. Г.А. Титоренко. – М.: ЮНИТИ-ДАНА, 2008. – 439 с.

4 Корнеев И. К. Информационный технологии учеб./ И. К. Корнеев, Г. Н. Ксандопуло, В. А. Машурцев – М.: ТК Велби, Изд-во Проспект, 2009. – 224 с.

5 Логинов В.Н. Информационные технологии управления: учебное пособие / В.Н. Логинов. – М.: КНОРУС, 2008. – 240 с.

6 Федотова Е.Л. Информационные технологии и системы: учеб. пособие / Е.Л. Федотова – М.: ИД «ФОРУМ»: ИНФРА-М, 2009. – 352 с.

7 Рогозин В.Ю. Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В.Ю. Рогозин. — М.: ЮНИТИ-ДАНА, 2017. – 287 c.

8 Галатенко В.А. Основы информационной безопасности / В.А. Галатенко. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 c.

9 Башлы П.Н. Информационная безопасность и защита информации: учебное пособие / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова.— М.: Евразийский открытый институт, 2012. – 311 c.

10 Дождиков В.Г. Краткий энциклопедический словарь по информационной безопасности / В.Г. Дождиков, М.И. Салтан. — М.: Энергия, 2010. – 239 c.