Менеджмент информационной безопасности.

Бакалавриат.

Учебное пособие

Данное пособие посвящено обеспечению безопасности компьютерных систем. Рассматриваются общие вопросы компьютерной безопасности, элементы безопасного хранения информации. Подробно рассмотрены уязвимости и угрозы безопасности, правовые аспекты организации защиты.

Рассмотрена возможность использования комплексной защиты для повышения эффективности защиты информации. Приведены примеры определения энтропии информации.

Пособие может быть рекомендовано студентам высших учебных заведений по направлениям подготовки бакалавров, связанным с компьютерной безопасностью, а также всем, кто стремится реализовать себя в сфере информационных систем и технологий.

Введение

Целью данного пособия является осуществление помощи обучающимся в приобретении необходимых теоретических знаний и практических навыков, методов и средств обеспечения защиты информации компьютерных систем и сетей в части вредоносного программного обеспечения.

В соответствии с ФГОС задачами изучения материала являются:

- научиться определять угрозы безопасности;
- выявлять уязвимые места компьютерных систем и обеспечивать их защиту;
- освоить современные методы и средства обеспечения защиты информации в компьютерных информационных системах.
- выбирать требуемые программные продукты для защиты от вредоносного программного обеспечения;
- понимать перспективы развития технологий защиты информации.

Курс предназначен для учащихся высших учебных заведений, которые стремятся реализовать себя в сфере информационных систем и технологий.

Курс дает возможность получить знания по обеспечению защиты информации и применить их на практике.

Требования к уровню освоения курса:

1. Знать:

- сущность и содержание дисциплины «Основы защиты информации»;
- основные законодательные и нормативно-правовые акты в области обеспечения защиты информации;
- основные типы и виды вредоносного программного обеспечения;
- основные виды сетевых угроз и атак;
- методы обеспечения информационной безопасности компьютерных систем;
- виды антивирусных программ;

- принципы функционирования антивирусных программ;
- общий алгоритм обнаружения неизвестного вируса;

2. Уметь:

- использовать основные современные средства обнаружения вредоносного программного обеспечения;
- определять вирусоподобные программы по основным признакам;
- классифицировать антивирусные программы;
- проводить профилактику вредоносного программного обеспечения;

3. Иметь представление:

- об истории возникновения проблем, связанных с компьютерной безопасностью;
- о юридических основах обеспечения защиты информации;
- о перспективах технологий обеспечения защиты информации.

1. Обеспечение защиты информации. Исходные математические понятия и факты, правовые аспекты информационной безопасности

1.1. Основные термины и определения

Основные положения по обеспечению защиты информации приведены в следующих документах:

- Закон Российской Федерации от 06.04.11 № 63-ФЗ «Об электронной подписи».
- Закон Российской Федерации от 04.05.11 № 99-ФЗ «О лицензировании отдельных видов деятельности»
- Закон Российской Федерации от 27.07.06 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Закон Российской Федерации от 07.07.03 № 126-ФЗ «О связи».

- Закон Российской Федерации от 21.07.93 № 5485-1 «О Государственной тайне».
- Закон Российской Федерации от 29.06.15 № 162-ФЗ «О стандартизации в Российской Федерации».
- Закон Российской Федерации от 17.01.97 № 85-ФЗ «Об участии в международном информационном обмене».
- Закон Российской Федерации от 27.07.06 № 152-ФЗ «О персональных данных».
- Приказ ФАПСИ от 13.06.01 № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
- Гражданский кодекс Российской Федерации.

Основные термины и определения сформулированы в следующих стандартах:

- ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
- ГОСТ Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения».
- ГОСТ Р 50.1.053-2005 «Информационная технология. Основные термины и определения в области технической защиты информации».

Основные термины, относящиеся к обеспечению защиты информации (в алфавитном порядке):

- *spyware* – программа, которая скрытным образом устанавливается на компьютер с целью сбора информации о конфигурации компьютера, пользователе, пользовательской активности или выполнения иных действий без согласия последнего.

- *антивирусная программа* – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.
- *безопасность автоматизированной информационной системы* – состояние защищенности автоматизированной информационной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчетность и подлинность ее ресурсов.
- *безопасность информации* – состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность (безопасность информации определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии).
- *безопасность информации (при применении информационных технологий)* – состояние защищенности информационной технологии, обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.
- *ботнет* – это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами – автономным программным обеспечением. Чаще всего *бот* в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера (рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании и так далее).
- *бэкдор* – программа, которая устанавливается взломщиками на компьютере после получения первоначального доступа с целью повторного получения доступа к системе.

- *вредоносная программа* – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.
- *доступность информации* – состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие соответствующие права доступа, могут беспрепятственно реализовывать их. К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации; права на изменение, использование и уничтожение ресурсов.
- *загрузочный вирус* – компьютерный вирус, записывающийся в первый сектор гибкого или жёсткого диска и выполняющийся при загрузке компьютера.
- *кейлогер* – программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя.
- *компьютерная атака* – целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.
- *компьютерный вирус* – это вредоносная программа, способная создавать вредоносные программы и (или) свои копии.
- *конфиденциальность информации* - необходимость предотвращения утечки (разглашения) какой-либо информации.
- *макровирус* – разновидность компьютерных вирусов, разработанных на макроязыках, встроенных в прикладные пакеты программного обеспечения.
- *полиморфный компьютерный вирус* – специальная техника, используемая авторами вредоносного программного обеспечения для снижения уровня детектирования вредоносной программы классическими антивирусными продуктами (не имеет сигнатур).

- *программное воздействие* – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.
- *руткит* – набор программных средств для обеспечения маскировки объектов, контроля событий, происходящих в системе, сбора данных о параметрах системы.
- *сетевая атака* – компьютерная атака с использованием протоколов межсетевого взаимодействия.
- *стелс-вирус* – вирус, полностью или частично скрывающий свое присутствие в системе, путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах.
- *файловый вирус* – компьютерный вирус, распространяющийся путем внедрения своего кода в тело исполняемых файлов.
- *целостность информации* – состояние информации (ресурсов автоматизированной информационной системы), при котором её (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право.

1.2. Понятие защиты информации

В настоящее время существуют разные определения понятия «информация». Данный термин ассоциируется с понятиями: сведения, данные, знания, известие, сообщение и тому подобный. Особенность информации состоит в том, что проявляется она только при взаимодействии объектов, которые представляют собой организованную структуру. Обычно предполагается наличие двух объектов хранения информации – источника информации и приемника (потребителя) и нестационарного, то есть изменяющегося во времени, процесса ее передачи от первого ко второму посредством передающего и приемного устройств (рис. 1.1).

Источник информации – это субъект или объект, порождающий информацию и представляющий ее в виде *сообщения*. *Приёмник информации* – это субъект или объект, принимающий *сообщение* и способный его интерпретировать. В этих определениях под словосочетание «субъект или объект» означает, что источник и приемник информации могут быть как неодушевленными (бумага, технические устройства), так и одушевленными (человек, общество).

Процесс передачи информации связан с физическим процессом, несущим информацию о событии или состоянии объекта наблюдения и называемым *сигналом*. Однако одиночный сигнал не может содержать большой объем информации. Поэтому для передачи обычно используется последовательность сигналов, называемая *сообщением*. Следовательно, сообщение служит переносчиком информации.

Под *компьютерной безопасностью* понимают состояние защищенности вычислительных устройств и компьютерных сетей.

Политика безопасности – это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.

Угроза защиты информации – событие или действие, которое может вызвать изменение функционирования компьютерной системы, связанное с нарушением защищенности обрабатываемой в ней информации.

Атака – реализация угрозы защиты информации, которая заключается в поиске и использовании той или иной уязвимости.

Угрозы защиты информации могут быть разделены на естественные

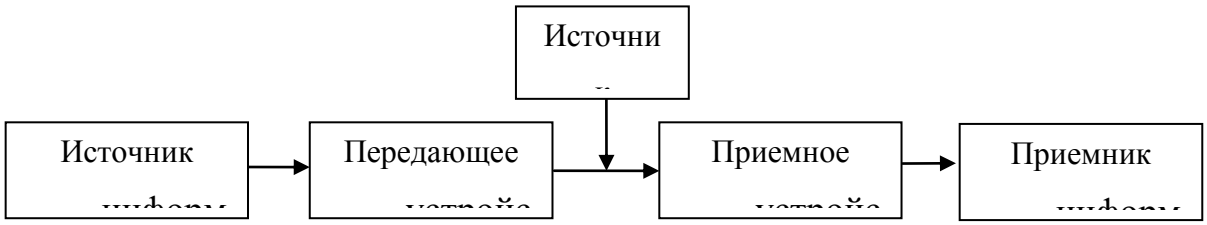

Рис. 1.1. Общая схема передачи информации.

угрозы, не зависящие от деятельности человека, и искусственные угрозы, вызванные человеческой деятельностью.

Искусственные угрозы делятся на *непреднамеренные* (случайные) и *преднамеренные* (умышленные).

К непреднамеренным угрозам относятся ошибки в проектировании систем, в разработке программных средств, случайные сбои в работе аппаратных средств, ошибки пользователей, воздействие электромагнитных полей других устройств и так далее.

К преднамеренным угрозам относятся кроме несанкционированного доступа к ресурсам также и несанкционированные действия обслуживающего персонала, в том числе ослабление политики безопасности, несанкционированный доступ к ресурсам КС.

Преднамеренные угрозы защиты информации делятся:

- на угрозы нарушения конфиденциальности (утечки информации ограниченного доступа, в том числе параметров подсистемы защиты информации);
- угрозы нарушения целостности информации, хранящейся в компьютерной системе или передаваемой между ними;
- угрозы нарушения доступности информации, то есть отказа в обслуживании.

Утечка информации может происходить по косвенным каналам:

- использование подслушивающих устройств;
- дистанционное видеонаблюдение;
- перехват побочных электромагнитных излучений и наводок (ПЭМИН, TEMPEST, Transient Electromagnetic Pulse Emanation Standard)

и непосредственным каналам:

- хищение носителей информации;
- преднамеренное копирование файлов других пользователей;

- копирование носителей информации;
- сбор производственных отходов с информацией (бумажных и магнитных носителей);
- чтение остаточной информации после выполнения заданий других пользователей (областей оперативной памяти, удаленных файлов, ошибочно сохраненных временных файлов);
- намеренное использование для несанкционированного доступа к информации незаблокированных терминалов пользователей;
- маскировка под других пользователей путем похищения их идентифицирующей информации;
- незаконное подключение специальной регистрирующей аппаратуры к устройствам или линиям связи;
- злоумышленное изменение программ для выполнения ими несанкционированного копирования информации при ее обработке;
- злоумышленный вывод из строя средств защиты информации.

Наличие в системе значительного числа возможных каналов утечки информации обусловливает её уязвимость с точки зрения защиты информации.

Для обеспечения защиты информации необходимо применять системно-концептуальный подход, включающий целевую системность (защищенность информации рассматривается как составная неотъемлемая часть ее качества), пространственную системность (взаимосвязанность защиты информации во всех элементах системы); временную системность (непрерывность защиты информации), организационную системность (единство организации всех работ по защите информации и управления компьютерными системами).

Компьютерную безопасность необходимо комплексно обеспечивать на всех этапах жизненного цикла системы с применением всех доступных методов и средств.

При передаче информации приемник информации должен не только принимать сообщение, но и его интерпретировать. Правилом *интерпретации сообщения* называется соответствие между сообщением и содержащейся в нем информацией. Данное соответствие может быть однозначным или неоднозначным. Неоднозначность интерпретации может быть вызвана передачей информации посредством различных сообщений для одного и того же приемника (например, передача письмом или шифротекстом) или передачей одного и того же сообщения для различных приемников (например, для зарегистрированного пользователя и нарушителя). Также в процессе передачи сообщения от источника информации к приемнику информация может искажаться. Это возможно в случае наличия помех (шумов) самих технических устройств (источника или приемника).

Существующие методы и средства обеспечения защиты информации делятся на методы и средства организационно-правовой защиты, инженерно-технической защиты, криптографические и программно-аппаратные.

1.3. Энтропия информации

Для измерения количества информации в теории кодирования принят энтропийный подход. Он основан на том, что получении информации связано с уменьшением разнообразия или неопределенности (*энтропии*) системы. Неопределенность понимается в смысле того, насколько мало известно наблюдателю о рассматриваемой системе. При получении информации энтропия (неопределенность) уменьшается, то есть система становится более упорядоченной.

Так как информация – содержание сообщения, в результате которого уменьшается энтропия (неопределенность) системы, то для того, чтобы измерить количество информации I, необходимо уметь вычислять ее энтропию H.

$$I = H_1 - H_2,$$

где H_1 - энтропия системы до получения информации;

H_2 - энтропия системы после получения информации.

Энтропию можно рассматривать и как количество информации, которое необходимо получить, чтобы система перестала быть неопределенной $H_2 = 0$.

Рассмотрим дискретную систему, имеющую конечное множество возможных состояний $\{s_i\}$, $i = \overline{1,n}$. Будем полагать, что все состояния системы различны. Множество состояний системы $S = \{s_1, s_2, \ldots, s_n\}$ называется ее *алфавитом*. А сами состояния s_i, $i = \overline{1,n}$ называются буквами, символами или знаками алфавита.

Рассматриваемая система может в каждый момент времени принимать одно из состояний s_i. Различные состояния могут возникать с различной *вероятностью* p_i. Однако для каждого состояния s_i вероятность p_i фиксирована. Так как система обязательно находится в каком-то из своих состояний, то сумма вероятностей возникновения какого-то состояния равна единице:

$$\sum_{i=1}^{n} p_i = 1.$$

Рассмотрим систему с равновероятными состояниями ($\forall i, j \;\; p_i = p_j = \frac{1}{n}$, $i, j = \overline{1,n}$). Чем в большем количестве возможных состояний может находиться система, тем меньше информации несет каждое состояние (больше оставшаяся энтропия системы). Если количество возможных состояний системы равно 1, то неопределенность системы отсутствует.

С другой стороны, если рассмотреть две независимые системы α и β с количеством равновероятных состояний n_α и n_β, то общая неопределенность двух систем ($\alpha\beta$) больше неопределенности каждой отдельно взятой и равна сумме их неопределенностей.

Таким образом, функция *H*, являющаяся мерой неопределенности системы, должна удовлетворять следующим условиям:

- она должна монотонно (непрерывно) возрастать с увеличением возможных состояний системы *n*: $H \in C^0$ (требование непрерывности), $\lim_{n\to\infty} H(n) = \infty$;
- при $n = 1$ функция равна 0: $H(1) = 0$;
- должно выполняться требование аддитивности: $H(n_\alpha \cdot n_\beta) = H(n_\alpha) + H(n_\beta)$;

Так как количество состояний системы *S* положительно ($n \geq 1$), то указанным требованиям удовлетворяет логарифмическая функция с любым основанием, превышающим 1:

$$H = \log_k n.$$

Величина основания *k* определяет только масштаб или единицу измерения системы.

Указанная мера неопределенности – логарифмическая мера информации $k\log_2 n$ (мера Хартли) для систем с равновероятными состояниями была предложена американским ученым Ральфом Винтоном Лайоном Хартли в 1928 году. В зависимости от основания логарифма применяются следующие единицы измерения неопределенности:

- бит – $H = \log_2 n$;
- нат – $H = \ln n$;
- дит – $H = \lg n$.

Для системы с состояниями, возникающими с разной вероятностью, при вычислении энтропии следует также учитывать вероятность произошедшего события. Действительно, в ситуации, когда система принимает менее вероятное состояние (с меньшим значением p_i), то информация о системе становится больше, чем при более вероятном состоянии. Действительно, если температура

человека все время 36,6 градусов, то каждый новый момент времени несет небольшую информацию о свойствах организма. Когда же температура становится равной 38,3 градусам, то информация значительно возрастает (энтропия уменьшается).

Американский ученый Клод Шеннон обобщил понятие меры неопределенности *H* на случай системы *S*, когда состояния (символы алфавита) s_i имеют разную вероятность p_i:

$$H = -\sum_{i=1}^{n} p_i \log_k p_i .$$

Эта величина, характеризующая неопределенность, приходящуюся в среднем на одно состояние системы, называется *энтропией* дискретного источника информации.

Пример. Пусть система может находиться в одном из трех состояний, причем вероятности нахождения в первом и втором состояниях равны соответственно $p_1 = 0{,}4;\ p_2 = 0{,}1$. Найти энтропию системы.

Так как система может находиться в одном из трех состояний, а сумма вероятностей равна 1 ($p_1 + p_2 + p_3 = 1$), то вероятность нахождения системы в третьем состоянии равна $p_3 = 1 - 0{,}4 - 0{,}1 = 0{,}5$. Тогда $\log_2(p_1) = \log_2 0{,}4 = -1{,}32$, $\log_2(p_2) = \log_2 0{,}1 = -3{,}32$, $\log_2(p_3) = \log_2 0{,}5 = -1$ и энтропия *H* равна:

$$H = -(p_1 \cdot \log_2(p_1) + p_2 \cdot \log_2(p_2) + p_3 \cdot \log_2(p_3)) =$$
$$0{,}4 \cdot 1{,}32 + 0{,}1 \cdot 3{,}32 + 0{,}5 \cdot 1 = 1{,}36 \text{ бит.}$$

Ответ: энтропия системы равна 1,36 бит.

1.4. Представление информации в технических устройствах

Для обеспечения защиты информации необходимо рассмотреть формы представления данных в технических устройствах. Не нарушая общности, можно рассматривать представление информации в дискретном виде, так как именно таким образом представленная информация обрабатывается компьютером и передается по различным линиям связи. Так как сообщение

представляет собой последовательность сигналов (знаков некоторого алфавита), то при передаче данных возникает проблема распознавания знака. Требуется прочитать сообщение, то есть по полученным сигналам восстановить исходную последовательность знаков первичного алфавита. Для этого проводится анализ получаемой информации.

В общем случае информация, которая содержится в сообщении, может зависеть от того, в какой момент времени оно получено. Однако в ряде сообщений информация не зависит от конкретного времени его получения. Например, при передаче данных посредством вычислительной техники, с точки зрения принимающего устройства определенный знак всегда остается тем же знаком. То есть такая ситуация реализуется, когда вероятность встретить какой-либо знак в сообщении одинакова во все моменты времени. Обычно в этом случае вероятность равна относительной частоте этого знака во всей последовательности знаков. В таблицах приведены относительные вероятности употребления букв русского и английского языков.

Буква	Вероят-ность	Буква	Вероят-ность	Буква	Вероят-ность	Буква	Вероят-ность
Пробел	0,175	Р	0,04	Я	0,018	Х	0,009
О	0,09	В	0,038	Ы	0,016	Ж	0,007
Е, Ё	0,072	Л	0,035	З	0,016	Ю	0,006
А	0,062	К	0,028	Ь, Ъ	0,014	Ш	0,006
И	0,062	М	0,026	Б	0,014	Ц	0,004
Т	0,053	Д	0,025	Г	0,013	Щ	0,003
Н	0,053	П	0,023	Ч	0,012	Э	0,003
С	0,045	У	0,021	Й	0,01	Ф	0,002

Буква	Вероят-ность	Буква	Вероят-ность	Буква	Вероят-ность
Пробел	0.2	H	0.047	W	0.012
E	0.105	D	0.035	G	0.011
T	0.072	L	0.028	B	0.01
O	0.065	C	0.023	V	0.008
F	0.063	F	0.023	K	0.003
N	0.058	U	0.023	X	0.001
I	0.055	M	0.021	J	0.001
R	0.052	P	0.018	Q	0.001
S	0.052	Y	0.012	Z	0.001

Энтропия, приходящаяся в среднем на каждый знак русской буквы, составляет, согласно формуле (2.3), 4,36 бит, а на каждый знак английской

буквы – 4,04 бита, французской – 3,96 бит, немецкой – 4,10 бит. Несовпадение значений энтропии для различных языков связано как с различным количеством букв языка, так и с различной вероятностью появления одних и тех же букв.

Сообщения, в которых вероятность появления каждого отдельного знака не меняется со временем, называются шенноновскими, а порождающий их отправитель – шенноновским источником.

Если сообщение является шенноновским, то набор знаков (алфавит) и информация, связанная с каждым из знаков, известны заранее. В этом случае интерпретация сообщения сводится к распознаванию конкретных знаков. Теория информации строится только для шенноновских сообщений.

В приведённых относительных вероятностях со средней информацией, приходящейся на буквы различных языков, были учтены вероятности появления букв в сообщениях. Однако если рассматривать не отдельные буквы, а их сочетания, то можно заметить, что некоторые из них вообще не встречаются. Например, в русском языке нет слов, содержащих пары *щц* и *фъ*. С другой стороны, некоторые сочетания встречаются более часто, а после, например, пары *пр* всегда следует гласная буква. Последовательность энтропий при учете возрастающего количества сочетаний является убывающей и стремится к некоторой величине $H_{\min}$, характеризующей минимальную неопределенность информации. Максимального значения энтропия достигает, как следует из ее свойств, при равной вероятности появления знаков алфавита.

Шеннон ввел величину, характеризующую рациональность применения символов алфавита, которую назвал избыточностью языка системы:

$$R = 1 - \frac{H_{\min}}{H_{\max}}.$$

Избыточность равна нулю только в случае независимости и равной вероятности знаков языка и максимальна при минимальном значении энтропии системы. Так как реальные системы могут находиться более чем в одном

состоянии, то их энтропия не может быть равна нулю, и, следовательно, избыточность всегда принимает значения меньше единицы.

При измерении информации в битах, выражение для избыточности можно записать в следующем виде:

$$R = 1 - \frac{H_{\min}}{\log_2 n},$$

где n – количество знаков в алфавите языка.

Пример. Определить избыточность языка (в процентах), состоящего из четырех символов: *а*, *б*, *в*, *г*, если вероятности их появления составляют: $p_a = 0{,}6;\ p_a = 0{,}25;\ p_a = 0{,}1;\ p_a = 0{,}05.$

Энтропия системы равна:

$$H = -0{,}6 \cdot \log_2 0{,}6 - 0{,}25 \cdot \log_2 0{,}25 - 0{,}1 \cdot \log_2 0{,}1 - 0{,}05 \cdot \log_2 0{,}05 =$$
$$0{,}44 + 0{,}50 + 0{,}33 + 0{,}22 = 1{,}49 \text{ бит.}$$

$$R = 1 - \frac{1.49}{\log_2 4} = 1 - 0{,}745 = 0{,}255.$$

В процентах избыточность языка составляет $R = 0{,}255 \cdot 100\% = 25{,}5\%.$

Ответ: избыточность языка составляет 25,5%.

Избыточность языка показывает, какую долю лишней информации содержат тексты данного языка. Исследования Шеннона показали, что для английского языка $H_{\min} = 1{,}45$ бит. То есть его избыточность составляет $R = 1 - \frac{1{,}45}{4{,}75} = 0{,}69$, то есть 69%. Это означает, что английский текст можно сократить практически в три раза без ущерба для его содержательной стороны и выразительности. Однако это привело бы к значительному уменьшению разборчивости языка и ухудшению его распознавания при наличии шумов. При этом передача информации, связанная с битовыми сообщениями, подразумевает равновероятное распределение информации, о чём будет сказано в разделе 3.

Чем больше избыточность, тем меньше требуется ресурсов линий связи при передаче сообщений, однако тем сложнее восстановить текст в случае ошибок при передаче. В этом смысле избыточность является определенной страховкой и гарантией разборчивости сообщений.

1.5. Задачи для самостоятельного решения

Задание. Имеются две системы, каждая из которых характеризуется двумя состояниями. Первая система находится в состоянии 1 с вероятностью 0,25, а вторая – 0,5. Вычислить энтропию систем? (0,81 бит, 1,0 бит)

Задание. Имеются два ящика (системы), в каждом из которых находится по 8 шаров двух цветов. В первом ящике 2 зеленых шара и 6 желтых шаров, а во втором – по 4 шара каждого цвета. Из каждого ящика вытаскивают по одному шару. Что можно сказать о неопределенностях опытов? (Так как энтропия (неопределенность) второй системы больше, чем первой, то предсказать исход опыта для второго ящика сложнее.)

Контрольные вопросы

1. Какие федеральные законы регламентируют деятельность по обеспечению защиты информации?
2. Что понимают под термином «информация»?
3. Что такое источник информации, приёмник информации?
4. Дайте определение защиты информации.
5. Чем определяется политика безопасности?
6. Что такое угроза защиты информации?
7. Приведите пример естественных и искусственных угроз защиты информации.
8. К какому типу угроз относятся непреднамеренные?
9. Перечислите виды преднамеренных угроз защиты информации.
10. Приведите пример непосредственных и косвенных каналов утечки информации.

11. Что такое энтропия?

2. Защита программного обеспечения

2.1. Угрозы защиты информации

Официальное определение компьютерного вируса и вредоносной программы было дано выше в п. 1.1. По своей сути, компьютерный вирус – вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения. По-видимому, впервые слово «вирус» по отношению к программе было употреблено в 1970 году американским астрофизиком и писателем-фантастом Грегори Бенфордом в фантастическом рассказе «Человек в шрамах». Коварство вирусов заключается в том, что его практически невозможно обнаружить до того момента, как он начинает свою вредоносную деятельность. При этом он постоянно совершенствуется и видоизменяется, находя новые способы проникновения на компьютеры пользователей. Необходимость борьбы с компьютерными вирусами определяется их возможностью нарушать информационную безопасность практически на всех этапах.

Компьютерные вирусы делятся на программные вирусы и вирусы, определяющие вирусную эпидемию. Компьютерные вирусы – это одна из главных угроз защиты информации. Это связано как с масштабом распространения данного явления, так и с огромным ущербом, наносимым различным информационным системам.

Компьютерные вирусы являются одной из наиболее распространенных причин нарушения конфиденциальности, целостности и доступности информации. Вирусные эпидемии способны блокировать эффективную

деятельность организаций и предприятий. Сегодня создание вирусов в основном является не столько хулиганством, сколько серьёзным бизнесом, коррелирующим с распространением спама, а также другими видами противозаконной деятельности. Несмотря на существование значительного количества компаний, занимающихся созданием антивирусов, убытки от компьютерных вирусов продолжают расти, вирусные эпидемии приобретают угрожающий характер. При этом, так как антивирусные программы являются только программным средством защиты, то они не дают гарантии защиты информации.

Основой компьютерного вируса является возможность их спонтанного произвольного по времени внедрения в различные компоненты операционной системы. Также особенностью вируса является способность создавать свои дубликаты и их модификации и внедрять их в коммуникационные системы, сети или файлы, системные области компьютера и прочие выполняемые объекты. Следует отметить, что возможность внедрения в операционную систему характерна не только для программ-вирусов. Однако программы, не относящиеся к данному классу, выполняют полезную с точки зрения функционирования системы работу.

Основной угрозой вируса с точки зрения защиты информации является отсутствие четких признаков, согласно которым можно однозначно отделить вирус от прочих программ. Поэтому на настоящий момент невозможно обеспечить компьютерную безопасность только с помощью защиты от вирусов. Для этой цели необходимо использовать комплексный набор аппаратных и программных средств различного спектра действия.

Для того чтобы полнее представлять возможности компьютерных вирусов и их функциональные возможности на данный момент следует понимать историю их возникновения и развития.

Основы теории самовоспроизводящихся механизмов и метод их создания были заложены американцем Джоном фон Нейманом в 1951 году. Первой

публикацией (1957), посвящённой созданию самовоспроизводящихся систем, стала статья английского учёного, нобелевского лауреата по физике Роджера Пенроуза, в которой была приведена информация о самовоспроизводящихся механических структурах, а также двумерная модель подобных структур, способных активизироваться, осуществить захват и осуществить освобождение. Данная статья послужила толчком к созданию биокибернетической модели, которая двигалась и «питалась» ненулевыми словами, что позволяло ей размножаться. При этом новые копии были подвержены процессу мутации. Отсутствие возможности питаться в течение длительного времени приводило к смерти копии.

В конце XX века с развитием компьютерной техники появляется большое количество программ. Чуть позже начинают активно развиваться компьютерные сети, что приводит к появлению различных вредоносных программ, так называемых «троянских коней», которые активизировались при запуске операционной системы. Одним из наиболее известных вирусов того времени стал вирус Brain (1986), который распространялся посредством дискет.

В 1987 году Ральф Бюргер опубликовал в своей книге по компьютерной вирусологии «Computer Viruses: A High Tech Desease» код вируса Vienna, что популяризировало процессы написания вирусов. Первые вирусы в основном были направлены на уничтожение информации, расположенной на компьютерах. В 1988 году была предпринята соответствующая акция в ряде университетов различных стран мира, которая пришлась на пятницу 13-е. Вирус быстро распространялся посредством компьютерных сетей.

Одним из наиболее разрушительных вирусов того времени явился вирус Internet Worm, который имел ошибку в коде. Это привело к неограниченной рассылке его копий по сетям и поглощению ресурсов компьютеров, что практически полностью блокировало их работу.

В 1992 году появился первый вирус, заражающий файлы операционной системы Windows. В дальнейшем возникает индустрия по созданию вирусов.

Несмотря на то, что растёт количество антивирусных программ (первая из которых появилась в 1985 году), а в 1994 году производится первый арест автора вируса, вирусы становятся всё более и более разнообразными.

В 1995 году появился первый вирус для Microsoft Word – макровирус Concept. Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносятся из одного зараженного файла в другие. Большая часть таких вирусов написана для MS Word.

С середины 90-х годов большая часть вирусов распространяется с помощью сети Internet. В 1998 году появились полиморфные вирусы, способные формировать код программы по мере работы вируса. Наиболее известным из них является Win95. CIH, который пересылался посредством интернет-конференций.

В конце XX века вирусная активность идёт на убыль, так как механизмы создания и распространения вирусов становятся более стандартными, что позволяет антивирусным компаниям и массовому пользователю снизить уровень возникновения угрозы. Однако последний год этого века ознаменовался появлением ряда новых типов вирусов. К ним относятся сетевой червь, супервирус и почтовый вирус.

Сетевой червь – вид вируса, который умеет самостоятельно распространяться через локальные и глобальные компьютерные сети.

Особенность супервируса Чернобыль является то, что он размещает свои фрагменты между фрагментами кода заражаемого файла, поэтому исходный размер заражённого файла не меняется, и сложно определить не только факт инфицирования, но и конкретный объект. Функционирование такого вируса возможно только под теми операционными системами, структура хранения файлов которых предполагает деление на блоки постоянного размера. К таким относится, например, ОС Windows. Также супервирус является первым вирусом, который способен изменять данные ПЗУ, то есть аппаратные средства.

Почтовый вирус LoveLetter распространялся с помощью программы арбы с электронной почтой Microsoft Outlook. Чтение письма, заражённого данным вирусом, активировало рассылку данного вируса по всем адресам электронной почты нового владельца от его имени. Атаке подверглось более 40 миллионов компьютеров.

В XXI веке появились так называемые «бестелесные черви», которые в момент передачи с одного компьютера на другой представляют собой сетевые пакеты, а внутри зараженного компьютера располагаются в оперативной памяти в виде программного кода, то есть в процессе функционирования не используют файлы.

В настоящее время среди вредоносного программного обеспечения преобладают различные виды сетевых червей, которые используют почтовые серверы для распространения.

2.2. Классификация вредоносных программ

В настоящее время не существует единой системы классификации и именования вирусов. Принято классифицировать вирусы в зависимости:

- от поражаемых объектов (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);
- механизма заражения (паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом);
- поражаемых операционных систем и платформ (DOS, Microsoft Windows, Unix, Linux);
- технологий, используемых вирусом (полиморфные вирусы, стелс-вирусы, руткиты);
- языка, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и другие);

- вида деструктивной деятельности (бэкдоры, кейлоггеры, шпионы, ботнеты и другие).

По среде обитания вирусы делятся на файловые, загрузочные, макровирусы и сетевые.

Файловые вирусы заражают выполняемые файлы, создают файлы-двойники (компаньон-вирусы) или используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы внедряются в загрузочный сектор диска (boot-сектор), в сектор, содержащий системный загрузчик жесткого диска (Master Boot Record) или меняют указатель на активный boot-сектор.

Макровирусы нарушают файлы-документы и электронные таблицы популярных офисных приложений.

Сетевые вирусы определяются средой распространения, которой служат протоколы или команды компьютерных сетей и электронной почты.

Также вирусы могут иметь смешанную среду обитания. Так, файлово-загрузочные вирусы могут заражать как файлы, так и загрузочные секторы дисков и чаще всего имеют сложный алгоритм работы с использованием стелс- и полиморфик-технологий. Сетевой макровирус, имея целью заражения редактируемые документы, распространяется при этом посредством почтовых программ.

Также вирусы делятся по применимости их в определённых операционных системах (одной или нескольких) или программах (MS Word, MS Excel и так далее), конкретных форматах расположения системных данных в загрузочных секторах дисков.

По особенностям алгоритма работы вирусы делятся на резидентные, стелс-вирусы, полиморфик-вирусы и вирусы, использующие нестандартные приемы.

Резидентный вирус имеет, как правило, две части, одна из которых сохраняется в оперативной памяти компьютера с последующим перехватом обращения операционной системы к предполагаемым объектам заражения,

после чего вторая часть внедряется в данные объекты. Резидентные вирусы, располагаясь в оперативной памяти, являются активными только до выключения или перезагрузки компьютера. К резидентным вирусам относятся макровирусы, так они присутствуют в памяти компьютера в течение времени работы с текстовым редактором, который играет роль операционной системы.

Стелс-алгоритмы скрывают своё присутствие с помощью перехвата обращений к операционной системе при чтении и/или записи заражённых файлов. При работе антивируса стелс-вирусы или временно лечат файлы, или маскируются, подставляя вместо себя незараженные участки.

Практически все типы вирусов используют самошифрование и полиморфичность для того, чтобы максимально усложнить процедуру их выявления. Полиморфик-вирусы не имеют сигнатур, то есть не содержат ни одного постоянного участка кода, что усложняет их обнаружение. Чаще всего два экземпляра одного и того же полиморфик-вируса не имеют ни одного совпадения в силу шифрования основного тела вируса и модификациями расшифровщика.

К нестандартным приемам относится процесс сокрытия вирусом себя в ядре операционной системы, защита резидентной копии, что затрудняет лечение.

По деструктивным возможностям вирусы условно делятся на безвредные, неопасные, опасные и очень опасные.

Безвредные вирусы практически не влияют на работу компьютера. Однако иногда вирус, который кажется безвредным, может активизироваться впоследствии и перейти в одну из следующих категорий.

Присутствие неопасных вирусов практически не проявляется, однако они занимают память и, тем самым, уменьшают свободное пространство.

Опасные вирусы могут привести к различным сбоям в работе компьютера, однако не нарушают целостность данных, программных и аппаратных средств.

Очень опасные вирусы могут привести к потере некоторых программ, уничтожить произвольные или конкретные данные, удалить необходимую для работы компьютера системную информацию, повредить аппаратные средства компьютера.

К вредоносным программам кроме вирусов также относят программы, которые сами по себе не являются вирусами, однако могут их создавать, помогают внедряться или маскироваться. К ним относят: Spyware (шпионские программные продукты), Keylogger, логические бомбы, троянские программы, сетевых червей, Ransomware.

- Spyware – программа, которая скрытным образом устанавливается на компьютер. Целью данной программы является несанкционированный сбор информации о различных параметрах компьютера, пользователе и его активности. Также такие программы могут производить и другие действия: изменение настроек компьютера, самостоятельная установка программ, перенаправление действий браузеров и так далее. Разновидностью Spyware является программа Adware, которая демонстрирует рекламу с согласия или без согласия пользователя. Такие программы не являются spyware в полной мере, но могут действовать скрытно.
- Keylogger – это программное обеспечение или аппаратное устройство, фиксирующее различные действия пользователя на клавиатуре и мыши.
- Логическая бомба – программа, которая самозапускается при выполнении определённых условий для осуществления вредоносных действий.
- Троянские программы – вредоносная программа, которая, в отличие от вирусов и червей, распространяется людьми. Это самый простой вид вредоносных программ, сложность которых зависит только от сложности задачи.
- Сетевые черви – разновидность вредоносной программы, которая самостоятельно распространяется через локальные и глобальные компьютерные сети.

- Ransomware – вредоносное программное обеспечение, используемое для вымогательства. В свое работе может осуществлять шифрование файлов, создавать помехи или полностью блокировать работу в системе и/или браузере.

Существуют различные классификации номенклатуры вредоносных программ. Чаще всего они делятся по вредоносной нагрузке и по методу размножения.

Вредоносная нагрузка в работе таких программ проявляется следующим образом:

- генерация помех в работе заражённого компьютера: уничтожение данных, блокировка антивирусного программного обеспечения, самопроизвольная работа внешних устройств;
- установка другого вредоносного программного обеспечения посредством распаковки другой программы или загрузки её из сети;
- шпионаж за пользователем с целью мошенничества, кражи или вымогательства путём фиксации нажатия клавиш, сканирования диска, перенаправления на вредоносные интернет-страницы путём сканирование жёсткого диска, регистрация нажатий клавиш и перенаправление пользователя на фальшивые сайты с целью блокировки компьютера, хищения конфиденциальной информации, в том числе аккаунтов служб и платёжных систем.
- другая незаконная деятельность, такая как получение несанкционированного доступа к различным ресурсам компьютера, использование техники для проведения DDoS-атак и тому подобное;
- показ рекламы, инициализация шуточного программного обеспечения, пересылка конфиденциальной информации, организация несанкционированного удалённого доступа и так далее, сокрытие другого программного обеспечения.

По методу размножения вредоносные программы подразделяют:

- на эксплойты, представляющие собой данные с ошибкой, из-за которой они некорректно воспринимаются специализированными программами, обрабатывающими такие данные;
- логические бомбы, срабатывающие при определённых условиях;
- троянские программы, которые не имеют собственного механизма размножения;
- компьютерные вирусы, размножающиеся в пределах компьютера, через сменные диски и через сеть при соответствующих действиях пользователя;
- сетевых червей, которые способны самостоятельно размножаться по сети.

Троянские программы и логические бомбы представляют собой программы, самозапускающиеся в зависимости от временных или других условий. Многие из таких программ маскируются под полезные программы или новые версии распространённых приложений.

Программы-шутки не являются вирусами и чаще всего используются для устрашения пользователя. Однако они способны нанести определённый вред, если, например, сообщают об обнаружении несуществующих вирусов в каких-либо пользовательских файлах.

Утилиты скрытого администрирования представляют собой вид логической бомбы, позволяющей совершать несанкционированное администрирование в компьютерной сети. В отличие от обычных программ они не предупреждают пользователя о попытке подключения к компьютеру, однако, как и легальные программы, позволяют осуществлять администрирование, то есть запуск других вредоносных программ, передачу конфиденциальной информации и так далее.

В настоящее время существуют вредоносные программы, которые не является вирусом, однако предназначены для их создания. Данные программы могут являться, например, в том числе логическими бомбами, которые в зависимости от конкретных условий осуществляют генерацию кода.

Полиморфизм компьютерных вирусных программ направлен на снижение возможности обнаружения вредоносного программного обеспечения за счёт видоизменения кода при каждом формировании новой копии вируса. Поэтому основной частью такого механизма является программный модуль, содержащий генератор новой копии.

Ряд вредоносных программ нельзя отнести к какому-то конкретному типу, так как они представляет собой цепочку. Например, это может быть эксплойт, который инициализирует программу-загрузчик, получающую данные посредством сети Интернет.

2.3. Угрозы безопасности

2.3.1. Классификация угроз безопасности

Угроза защиты информации – событие или действие, которое может вызвать изменение функционирования компьютерной системы, связанное с нарушением защищенности обрабатываемой в ней информации.

Угрозы делятся в зависимости:

- от источника угрозы;
- объекта воздействия;
- последствия реализации угрозы:
    - нарушения конфиденциальности информации;
    - нарушения целостности информации;
    - нарушения доступности информации.

Источник угрозы напрямую связан с характеристикой и потенциалом нарушителя, поэтому его принято классифицировать как внешнего или внутреннего нарушителя с низким, средним или высоким потенциалом.

Объектами воздействия могут быть аппаратное обеспечение, данные, виртуальная машина, микропрограммное и аппаратное обеспечение BIOS/UEFI, носители информации, объекты файловой системы и так далее.

Рассмотрим некоторые угрозы, связанные нарушением одновременно конфиденциальности, целостности и доступности информации.

К такому типу угроз относится угроза несанкционированного использования привилегированных функций BIOS. Угроза заключается в возможности использования нарушителем потенциально опасных возможностей BIOS/UEFI. Интересным фактором здесь является то, что такая угроза может исходить как от внешнего нарушителя с высоким потенциалом, так и от внутреннего нарушителя с низким потенциалом. То есть внутренним нарушителем может являться практически любой по потенциалу объект.

Аналогичной по модели нарушителя является и угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети. Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на виртуальные машины из виртуальной и (или) физической сети как с помощью стандартных (не виртуальных) сетевых технологий, так и с помощью сетевых технологий виртуализации. Данная угроза обусловлена наличием у создаваемых виртуальных машин сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами. Реализация данной угрозы возможна при условии наличия у нарушителя сведений о сетевом адресе виртуальной машины, а также текущей активности виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия

2.3.2. Классификация уязвимостей

Уязвимость – это недостаток в системе, используя который, можно злонамеренно инициировать неправильную работу системы, нарушить её целостность. Уязвимость может быть результатом различного рода ошибок, таких как ошибки программирования, ошибки проектирования системы, возможность ввода ненадежных паролей. Уязвимости используются вирусами и другим вредоносным программным обеспечением, скриптовыми и SQL-

инъекциями. Часть уязвимостей известны, но не используется (теоретические уязвимости), другая часть активно используется и может иметь известные эксплойты. Для обеспечения защиты информации проводится поиск и диагностика уязвимостей с целью предотвращения возможности их использования.

В настоящее время один из использующихся вариантов классификации угроз безопасности основан на базовых, временных и контекстных метриках.

Базовые метрики – метрики, отражающие основные характеристики уязвимости, влияющие на доступность, целостность и конфиденциальность информации, которые не изменяются во времени и не зависят от среды функционирования программного обеспечения.

К базовым метрикам относят следующие характеристики уязвимости:

- способ получения доступа;
- сложность получения доступа;
- аутентификация;
- влияние на конфиденциальность;
- влияние на целостность;
- влияние на доступность.

Способы получения доступа разделяются на локальные, по смежной сети и сетевые. Сложность получения доступа варьируется от низкой до высокой. Аутентификация может проводиться (делится на единственную и множественную) или не требоваться.

С точки зрения влияния на конфиденциальность, целостность и доступность вредоносное программное обеспечение определяется как полное, частичное или не оказывает по каждому из параметров.

Временные метрики – метрики, отражающие характеристики уязвимости, которые изменяются со временем, но не зависят от среды функционирования программного обеспечения.

К временным метрикам относят следующие характеристики уязвимости:

- возможность использования;
- уровень исправления;
- степень достоверности источника.

Возможность использования уязвимости может характеризоваться как высокая, согласно сценарию, согласно концепции, теоретическая или неопределённая.

Уровни исправления уязвимости делятся на недоступные, согласно рекомендации, временные, официальные и неопределённые.

Степень достоверности источника характеризуется как подтверждённая, недоказанная, неподтверждённая и неопределённая.

Контекстные метрики – это метрики, отражающие характеристики уязвимости, зависящие от среды функционирования программного обеспечения.

К контекстным метрикам относят следующие характеристики уязвимости:

- вероятность нанесения косвенного ущерба;
- плотность целей;
- требования к конфиденциальности;
- требования к целостности;
- требования к доступности.

Значения всех характеристик данной метрики варьируются от высокой до низкой с выделением в отдельный класс неопределённой вероятности или варианта «отсутствует». В зависимости от характеристики градация более или менее грубая.

В зависимости от значений указанных характеристик можно сделать вывод о критичности уязвимости.

Наибольшее количество уязвимостей относится к операционным системам.

По типам ошибок наибольшее количество уязвимостей диагностируется с ошибкой CWE-119, что характеризует выполнение операций, связанных с буфером памяти в части чтения или записи в ячейку памяти, которая находится за пределами предполагаемой границы буфера.

Для устранения уязвимостей используется статический и динамический анализ кода. Известные уязвимости группируются в классы с возможностью их пополнения. На основе этого можно провести локализацию и устранение ошибок проектирования программного обеспечения.

Контрольные вопросы

1. Перечислите характерные черты вредоносного программного обеспечения.
2. Дайте определение компьютерного вируса.
3. Каковы причины распространения компьютерных вирусов?
4. Что является основой вируса с точки зрения защиты информации?
5. Почему невозможно обеспечить абсолютную компьютерную безопасность от вредоносного программного обеспечения?
6. Что такое сетевой червь?
7. В зависимости от чего принято классифицировать вирусы?
8. На какие типы делятся вирусы по среде обитания? Приведите примеры.
9. На какие типы делятся вирусы по особенностям алгоритма? Приведите примеры.
10. На какие типы делятся вирусы по деструктивным возможностям?
11. Что такое безвредные вирусы? Действительно они являются безвредными?
12. Что относится к вредоносному программному обеспечению кроме вирусов?
13. Что понимается под шпионским программным обеспечением?
14. Каковы свойства логической бомбы?

15. Поясните механизм работы троянской программы.

16. Сформулируйте признаки стелс-вирусов.

17. В чём может выражаться вредоносная нагрузка программного обеспечения?

18. На какие типы делятся вирусы по методу размножения? Приведите примеры.

19. Что такое угроза безопасности?

20. В зависимости от чего делятся угрозы?

21. Что такое уязвимость?

22. Каковы причины возникновения уязвимостей?

23. Что такое базовые, временные и контекстные метрики?

24. Какие характеристики уязвимостей относятся к базовым метрикам?

25. Какие характеристики уязвимостей относятся к временным метрикам?

26. Какие характеристики уязвимостей относятся к контекстным метрикам?

27. Зачем необходимо знать характеристики уязвимостей?

28. Как можно бороться с уязвимостями?

3. Обеспечение надежности хранения и передачи информации

3.1. Обеспечение надёжности при передаче информации

Организация хранения и передачи информации являются одним из наиболее важных этапов в защите от вредоносного программного обеспечения.

Передача информации может происходить внутри одного вычислительного устройства или между различными ЭВМ. В первом случае два потребителя (например, оперативная память и постоянное запоминающее устройство) связаны непосредственно кабелем. Такой же способ связи возможен и во втором случае, если устройства находятся недалеко друг от друга. При значительной же удаленности ЭВМ друг от друга связь, как правило, осуществляется посредством телефонных линий. Это диктуется в

основном экономическими соображениями, так как иначе потребовалось бы прокладывать специальные кабели значительной длины. Основная проблема, связанная с передачей информации по телефонным линиям, определяется формой представления сигнала. В компьютере сигнал является цифровым (дискретным), а телефонные линии работают с аналоговым (непрерывным) сигналом. То есть импульсный сигнал должен преобразовываться в аналоговый и обратно. Устройство, производящее такое преобразование, называется модемом. Название определяется его функциональным назначением: модуляцией («мо») сигнала в аналоговый и демодуляцией («дем») его обратно в импульсный. Соответственно передача сигнала от одного компьютера к другому происходит по следующей схеме: «Компьютер 1» - «Асинхронный преобразователь 1» - «Модем 1» - «Модем 2» - «Асинхронный преобразователь 2» - «Компьютер 2».

В компьютерных линиях используются два способа передачи информации: параллельный и последовательный.

При параллельном способе передачи информации передаются одновременно все биты машинного слова. То есть здесь требуется линия связи, в которой количество проводников соответствует количеству бит передаваемой и принимаемой информации. Такие линии называются шиной. Количество проводников определяет разрядность шины. В современных компьютерах обычно используются 16-разрядные шины. Шина обеспечивает наиболее быстрый способ передачи информации, так как за два такта синхрогенератора передается машинное слово целиком. Параллельная передача информации происходит, например, на материнской плате компьютера, между различными магнитными дисками, между компьютером и асинхронным преобразователем и так далее.

Для передачи информации на большие расстояния используется последовательный способ передачи информации. Он характеризуется

поочередной передачей бит, начиная с младшего. Возможны два режима последовательной передачи: синхронный и асинхронный.

При синхронной передаче каждый передаваемый бит сопровождается импульсом синхронизации, который сообщает о наличии в линии связи информационного бита. Таким образом, при синхронной передаче помимо непосредственно кабеля передачи информации должен существовать дополнительный кабель передачи синхроимпульсов. Такая передача оказывается целесообразной, только если расстояние между передаточным и приемным устройством невелико, и при этом передаются не отдельные символы, а массив символов. Поэтому синхронный способ передачи информации не имеет широкого распространения.

При асинхронной передаче информации синхронизация не требуется. Однако приемник и передатчик должны быть согласованы по формату (протоколу) и скорости. Передача производится машинными словами, дополненными несколькими служебными битами. Пересылка начинается после генерации передатчиком так называемого стартового бита. По нему приемник узнает, что началась передача информации. Затем передаются информационные биты, начиная с младшего, и контрольный бит четности. Передача заканчивается стоповым битом, который переводит линию в состояние ожидания. Передача следующей части информации может начаться в любой момент посылкой стартового бита, например, сразу после завершения предыдущей порции.

При передаче данных по последовательным линиям связи возможны три различные направленности передачи информационного канала:

- симплексный, когда передача по данному каналу возможна только в одну сторону;
- полудуплексный, при котором передача сигнала возможна в обе стороны, но не одновременно (в определенный момент времени она осуществляется только в одном направлении);

- дуплексный, когда связь в обоих направлениях обеспечивается одновременно.

Последовательный способ передачи информации используется при больших удалениях устройств друг от друга или при подготовке к такой передаче (например, при связи асинхронного преобразователя и модема).

3.2. Восстановление информации при обнаружении одиночной ошибки

При передаче (а иногда и при хранении) информации возможно возникновение ошибок, связанных с действием вредоносного программного обеспечения. В этом случае сначала необходимо ошибку обнаружить.

Вообще говоря, для обнаружения ошибки достаточно продублировать всю информацию. Тогда, если в двух версиях будет наблюдаться различие, то можно говорить о наличии ошибки. Например, если продублировать слово «мало», то храниться или передаваться должна последовательность «ммааллоо». Если же при получении будет обнаружена, например, последовательность «мсааллоо», то произошла ошибка. Однако такой способ приводит к значительному увеличению избыточности сообщения. Поэтому обычно используется другой способ.

Пусть передается некоторая последовательность двоичных знаков. Для обеспечения надежности передачи к ним добавляется еще один контрольный бит так, чтобы общая сумма бит (количество 1) была чётная – по этой причине этот контрольный бит также называется *битом чётности*. Тогда, если при передаче сумма бит четная, то ошибки не произошло, а если нечетная, то есть ошибка. Данный способ позволяет обнаружить одиночную ошибку сообщения.

Пример. Проверить, произошла ли ошибка при передаче информации 001001110 (бит четности выделен подчеркиванием).

Сумма полученных бит равна 4, что является четным числом. Поэтому ошибки не было.

Ответ: ошибки нет.

Данный способ позволяет обнаружить ошибку, но не исправить ее. Если сообщение невелико, то при обнаружении ошибки можно запросить информацию еще раз. Однако, если передача информации связана со значительными затратами, то это является экономически невыгодным. Поэтому иногда требуется не только обнаружить ошибку, но и ее исправить.

Для исправления одиночной ошибки также существует несколько способов. Если рассматривать дублирование информации, то здесь достаточно повторить ее не два, а три раза. Тогда при одиночной ошибке каждый символ будет передан три раза подряд (без ошибки) или в комбинации два и один (ошибка). В этом случае достаточно взять тот из них, который записан два раза.

Пример. Проверить, произошла ли ошибка при передаче информации «мммаиалллооо» и при необходимости ее исправить.

Символы «м», «л», «о» переданы три подряд, следовательно, без ошибки. В комбинации «аиа» символ «а» встречается два раза, значит исходно присутствовал именно он. Исходное сообщение: «мало».

Ответ: «мало».

Однако, если при двойном дублировании информации значительно возрастает избыточность сообщения, то при тройном – тем более. Метод кодирования информации для ее передачи с возможностью обнаружения и исправления одиночной ошибки был предложен Р. Хеммингом.

Для построения *кода Хемминга* используются несколько битов четности в одном сообщении. Если пронумеровать все биты слева направо в порядке возрастания, начиная с 1, то контрольными битами являются все, имеющие степень числа 2 (1, 2, 4, 8, 16 и так далее). При передаче восьми битов следующей информации «00101101» она будет распределена в сообщении следующим образом:

1	2	3	4	5	6	7	8	9	10	11	12
		0		0	1	0		1	1	0	1

7	6	5	4	3	2	1	0

где над таблицей указаны номера битов Хемминга, а под ней – информационные биты.

Правила формирования контрольных битов:

- первым контролируемым битом для бита с номером *n* является он сам;
- контрольный бит с номером *n* контролирует n бит подряд, после которых n бит не контролирует.

Например, контрольный бит 1 контролирует биты, начиная с первого, причем один контролирует, один нет. То есть он контролирует следующие биты: 1, 3, 5, 7 и так далее. Контрольный бит 2 контролирует биты, начиная со второго, причем два бита контролирует, а следующие два – нет. То есть он контролирует следующие биты: 2, 3, 6, 7, 10, 11 и так далее. В таблице по

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	▨		▨		▨		▨		▨		▨		▨		▨	
2		▨	▨			▨	▨			▨	▨			▨	▨	
4				▨	▨	▨	▨					▨	▨	▨	▨	
8								▨	▨	▨	▨	▨	▨	▨	▨	
16																▨

горизонтали указаны номера битов Хемминга, а по вертикали – номера контрольных битов. Закрашенные ячейки соответствуют контролируемым битам.

Контрольные биты формируются таким образом, чтобы суммарная контролируемая информация давала четное количество единиц.

Пример. Построить код Хемминга для последовательности «00101101».

Для данной последовательности распределение информационных битов для кода Хемминга представлено в таблице:

1	2	3	4	5	6	7	8	9	10	11	12
		0		0	1	0		1	1	0	1
		7		6	5	4		3	2	1	0

Контролирующий бит 1 отвечает за биты 1, 3, 5, 7, 9 и 11. Информация, содержащаяся в указанных битах (без бита 1), следующая: 0, 0, 0, 1, 0. Сумма равна 1 (нечетная), следовательно бит четности 1 должен быть равен 1.

Контролирующий бит 2 отвечает за биты 2, 3, 6, 7, 10 и 11. Информация, содержащаяся в указанных битах (без бита 2), следующая: 0, 1, 0, 1, 0. Сумма равна 2 (четная), следовательно бит четности 2 должен быть равен 0.

Контролирующий бит 4 отвечает за биты 4, 5, 6, 7 и 12. Информация, содержащаяся в указанных битах (без бита 4): 0, 1, 0, 1. Сумма равна 2 (четная), следовательно бит четности должен 4 быть равен 0.

Контролирующий бит 8 отвечает за биты 8, 9, 10, 11 и 12. Информация, содержащаяся в указанных битах (без бита 8): 1, 1, 0, 1. Сумма равна 3 (нечетная), следовательно бит четности 8 должен быть равен 1.

Таким образом, дополнив последовательность контрольными битами, получим:

1	2	3	4	5	6	7	8	9	10	11	12
1	0	0	0	0	1	0	1	1	1	0	1
		7		6	5	4		3	2	1	0

Ответ: 100001011101.

Для обнаружения ошибки необходимо при получении информации проверить биты четности. Если произошла ошибка, следует сложить номера битов четности, информирующих об ошибке. Итоговое число соответствует номеру бита, содержащего ошибку.

3.3. Задачи для самостоятельного решения

Задание. Проверить, произошла ли ошибка при передаче информации 101011010 (бит четности выделен подчеркиванием). (Ошибка есть.)

Задание. Проверить, произошла ли ошибка при передаче информации «100101011101» и при необходимости ее исправить.

Решение. Для контрольного бита 1 полученная информация имеет вид: 1, 0, 0, 0, 1, 0. Сумма четная. Ошибки нет.

Для контрольного бита 2 полученная информация имеет вид: 0, 0, 1, 0, 1, 0. Сумма четная. Ошибки нет.

Для контрольного бита 4 полученная информация имеет вид: 1, 0, 1, 0, 1. Сумма нечетная. Ошибка.

Для контрольного бита 8 полученная информация имеет вид: 1, 1, 1, 0, 1. Сумма четная. Ошибки нет.

Ошибка найдена только при проверке контрольного бита 4. Значит ошибка в бите 4. Передаваемая последовательность: 100001011101. Искомое сообщение 00101101.

Задание. Проверить, произошла ли ошибка при передаче информации «100001010101» и при необходимости ее исправить.

Решение. Для контрольного бита 1 полученная информация имеет вид: 1, 0, 0, 0, 0, 0. Сумма нечетная. Ошибка.

Для контрольного бита 2 полученная информация имеет вид: 0, 0, 1, 0, 1, 0. Сумма четная. Ошибки нет.

Для контрольного бита 4 полученная информация имеет вид: 0, 0, 1, 0, 1. Сумма четная. Ошибки нет.

Для контрольного бита 8 полученная информация имеет вид: 1, 0, 1, 0, 1. Сумма нечетная. Ошибка.

Ошибка найдена только при проверке контрольных битов 1 и 8. Значит ошибка в бите 9 (1+8=9). Передаваемая последовательность: 100001011101. Искомое сообщение 00101101.

Контрольные вопросы

1. Перечислите способы передачи информации. Приведите примеры.

2. Как организован параллельный способ передачи информации?

3. Что такое последовательный способ передачи информации? Когда он используется?

4. Перечислите режимы последовательной передачи информации.

5. В чём состоит асинхронная передачи информации?

6. Какие существую виды направленности передачи информации по последовательным линиям связи?

7. Что такое бит чётности? Зачем он используется? Можно ли его использовать для исправления ошибок при передаче информации?

8. Для чего используется код Хемминга?

Заключение

Невозможно обеспечить абсолютную безопасность компьютерных систем. Однако наиболее надежная защита может быть обеспечена комплексным применением аппаратных и программных средств.

Вредоносное программное обеспечение является одной из главных угроз информационной безопасности. Это связано с масштабностью распространения этого явления и, как следствие, огромного ущерба, наносимого информационным системам.

Вредоносное программное обеспечение делятся по среде обитания, по особенностям работы алгоритма, по деструктивным возможностям. Утилиты скрытого администрирования являются разновидностью троянских программ, которые используются злоумышленниками для удаленного администрирования компьютеров в сети. Конструкторы вирусов предназначены для создания новых компьютерных вирусов.

Основными путями проникновения вредоносного программного обеспечения в компьютеры являются глобальные и локальные сети и пиратское программное обеспечение.

Одним из наиболее эффективных способов борьбы с вирусами является использование антивирусного программного обеспечения. Наиболее эффективными антивирусными программами являются антивирусные сканеры и CRC-сканеры. Качество антивирусной программы определяется по их надёжности функционирования, универсальности, наличии резидентной части.

Библиографический список

1. Банк данных угроз безопасности информации. URL: http://www.bdu.fstec.ru. Дата обращения: 07.10.15.

2. Богомолова О.Б., Усенко Д.Ю. Защита компьютера от вредоносных воздействий: практикум. – М .: Бином. Лаборатория знаний, 2014. – 176 с.

3. Информационная безопасность. URL: http://www.itsec.ru/main.php. Дата обращения: 30.09.15.

4. Корпоративный журнал компании «Инфосистемы Джет». URL: http://www.jetinfo.ru. Дата обращения: 30.09.15.

5. Об угрозах. URL: http://www.kaspersky.ru/internet-security-center. Дата обращения: 30.09.15.

6. Применко Э.А. Алгебраические основы криптографии. – М.: Либроком, 2014. – 294 с.

7. Семенов А., Соловьев Н., Чернопрудова Е. и др. Интеллектуальные системы: учебное пособие. – Оренбург: ОГУ, 2013. – 236 с.

8. Хорев П.Б. Криптографические интерфейсы и их использование. – М.: Горячая линия-Телеком, 2007. – 158 с.

9. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2008. – 255 с.

10. Хорев П.Б. Программно-аппаратная защита информации. – М.: ФОРУМ, 2012. – 352 с.

Оглавление

Введение 2
1. Обеспечение защиты информации. Исходные математические понятия и факты, правовые аспекты информационной безопасности 3
1.1. Основные термины и определения 3
1.2. Понятие защиты информации 7
1.3. Энтропия информации 11
1.4. Представление информации в технических устройствах 14
1.5. Задачи для самостоятельного решения 18
2. Защита программного обеспечения 19
2.1. Угрозы защиты информации 19
2.2. Классификация вредоносных программ 23
2.3. Угрозы безопасности 29
2.3.1. Классификация угроз безопасности 29
2.3.2. Классификация уязвимостей 30
3. Обеспечение надежности хранения и передачи информации 34
3.1. Обеспечение надёжности при передаче информации 34
3.2. Восстановление информации при обнаружении одиночной ошибки 37
3.3. Задачи для самостоятельного решения 40
Заключение 42
Библиографический список 82