Тогда $0 \le q(t) \le q_0 = 1 - \ell L\varepsilon\left(\frac{2}{L} - \varepsilon\right) < 1$ и, следовательно, $E_S\left(\overline{W}(t)\right) \to E_S\left(\overline{W}^*\right)$ при $t \to \infty$.

В силу того, что для сильно выпуклой функции с константой ℓ выполняется: $E_S\left(\overline{W}\right) \ge E_S\left(\overline{V}\right) + \left(\nabla E_S\left(\overline{V}\right), \overline{W} - \overline{V}\right) + \frac{\ell}{2}\left\|\overline{W} - \overline{V}\right\|^2$, то, полагая $\overline{V} = \overline{W}^*$ и учитывая, что $\nabla E_S\left(\overline{W}^*\right) = \overline{0}$, получим

$$E_S\left(\overline{W}\right) \ge E_S\left(\overline{W}^*\right) + \frac{\ell}{2}\left\|\overline{W} - \overline{W}^*\right\|^2$$ или

$$\left\|\overline{W} - \overline{W}^*\right\|^2 \le \frac{2}{\ell}\left(E_S\left(\overline{W}\right) - E_S\left(\overline{W}^*\right)\right).$$

Откуда $\left\|\overline{W}(t) - \overline{W}^*\right\|^2 \le \frac{2}{\ell}\left(E_S\left(\overline{W}(t)\right) - E_S\left(\overline{W}^*\right)\right) \le$

$$\le \frac{2}{\ell} q_0^t \left(E_S\left(\overline{W}(0)\right) - E_S\left(\overline{W}^*\right)\right).$$

Таким образом, $\left\|\overline{W}(t) - \overline{W}^*\right\| \le cq^t$, где $c = \sqrt{\frac{2}{\ell}}$, $0 \le q = \sqrt{q_0} = \sqrt{1 - \ell L\varepsilon\left(\frac{2}{L} - \varepsilon\right)} < 1$, что и требовалось доказать.

Замечание. Использованная техника построения доказательств приведенных утверждений может быть распространена и на более широкий класс функций ошибки сети с получением локальных аналогов полученных теорем.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Головко В.А. Нейронные сети: обучение, организация и применение. Кн. 4: Учебное пособие для вузов / Общая ред. А.И. Галушкина. – М.: ИПРЖР, 2001. – 256 с.: ил. (Нейрокомпьютеры и их применение).
2. Гладкий И.И., Головко В.А., Махнист Л.П. Обучение нейронных сетей с использованием метода наискорейшего спуска // Вестник Брестского государственного технического университета. Физика, математика, химия. – Брест: БГТУ, 2001. – № 5 – С. 47-55.
3. Махнист Л.П. Обучение нейронных сетей с использованием метода сопряженных градиентов // Вестник Брестского государственного технического университета. Машиностроение, автоматизация, ЭВМ. – Брест: БГТУ, 2002. – № 4 – С. 74-77.

УДК 004.8.032.26

Головко В.А., Войцехович Л.Ю.

НЕЙРОСЕТЕВЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ АТАК НА КОМПЬЮТЕРНЫЕ СЕТИ

1. ВВЕДЕНИЕ

Одной из форм глобализации мирового пространства является информационная глобализация, которая связана с широким распространением сети Интернет. Информационная глобализация увеличивает степень уязвимости компьютерных систем, что уменьшает их безопасность. Атакой на компьютерные сети называется совокупность определенных действий, приводящих к подрыву безопасности системы. В результате атаки злоумышленник может получить доступ к конфиденциальной информации или нарушить нормальное функционирование системы. Это приводит к большим материальным и социальным издержкам.

Важным этапом обеспечения безопасности компьютерных систем является проектирование систем обнаружения атак (Intrusion Detection System – IDS). Такие системы способны на основе анализа сетевого трафика автоматически обнаруживать атаки TCP/IP, что позволяет предпринять необходимые меры для нейтрализации угрозы.

В данной работе рассматриваются нейросетевые подходы для построения систем обнаружения атак. В качестве базы данных для тестирования системы используется KDD-99 [1], которая содержит почти 5 миллионов записей соединений и 41 параметр сетевого трафика. При этом атаки делятся на четыре основные категории: DoS, U2R, R2L и Probe.

Атака DoS – отказ в обслуживании, характеризуется генерацией большого объема трафика, что приводит к перегрузке и блокированию сервера.

Атака U2R предполагает получение зарегистрированным пользователем привилегий локального суперпользователя (администратора).

Атака R2L характеризуется получением доступа незарегистрированного пользователя к компьютеру со стороны удаленной машины.

Атака Probe заключается в сканировании портов с целью получения конфиденциальной информации.

В работе предлагаются различные варианты построения систем обнаружения атак, которые базируются на использовании рециркуляционных и многослойных нейронных сетей. Результаты экспериментов обсуждаются.

2. ГЕНЕРИРОВАНИЕ АРХИТЕКТУРНЫХ РЕШЕНИЙ

Рассмотрим различные архитектурные решения для построения систем обнаружения атак. В качестве входных данных используется 41-размерный вектор, который характеризует параметры соединения сети. Задачей IDS является обнаружение и распознавание атак. Поэтому в качестве выходных данных используется m-мерный вектор, где m равняется количеству атак плюс нормальное состояние.

На рис. 1 приведена система обнаружения атак, которая состоит из рециркуляционной нейронной сети (RNN) и многослойного персептрона (MLP).

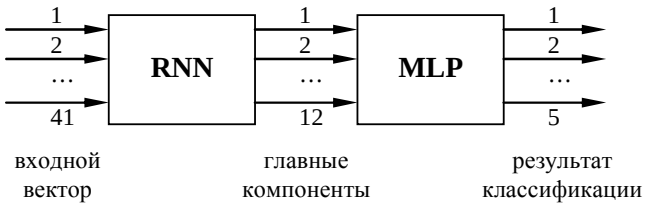


Рис. 1. 1-ый вариант IDS.

Задачей RNN является сжатие входного пространства образов с целью получения главных компонент [2]. Главные компоненты являются некоррелированными и содержат наиболее информативные признаки исходного пространства образов. Многослойный персептрон осуществляет обработку сжатого пространства входных образов (главных компонент) с целью распознавания типа атаки.

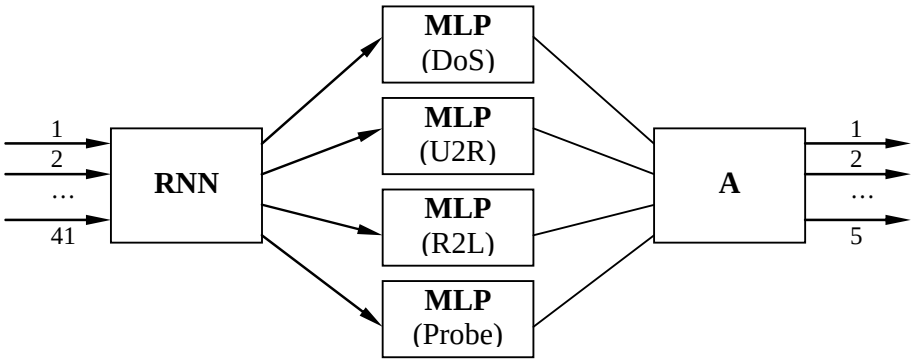


Рис. 2. 2-ой вариант IDS.

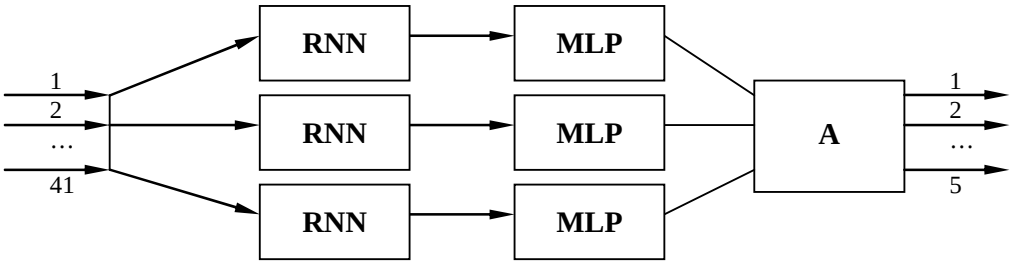


Рис. 3. 3-ий вариант IDS.

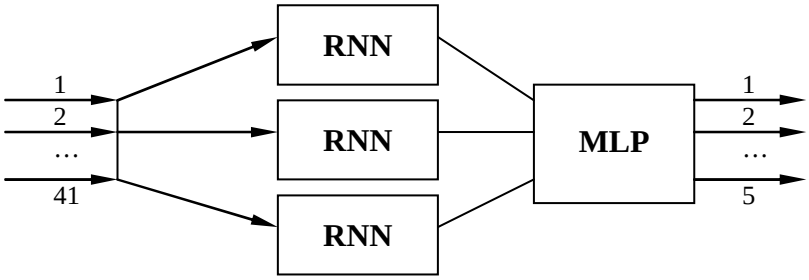


Рис. 4. 4-ый вариант IDS.

На рис. 2 приведена вторая схема системы обнаружения атак. Она характеризуется тем, что главные компоненты с выходов RNN одновременно поступают на 4 отдельных многослойных персептрона, каждый из которых соответствует определенному типу атаки: DoS, U2R, R2L и Probe. С выходов MLP данные поступают на арбитр, который и принимает окончательное решение о состоянии системы. В качестве арбитра может использоваться линейный или многослойный персептрон. Тогда обучение его будет производиться после обучения RNN и MLP. Такая схема может осуществлять иерархическую классификацию атак. В этом случае арбитр определяет один из 5 типов атаки, а соответствующий многослойный персептрон – класс атаки.

На рис. 3 изображен третий вариант IDS. Он характеризуется тем, что исходный 41-размерный вектор данных разбивается на части (подвекторы), содержащие однородные данные. При этом для каждого подвектора ставится в соответствие своя RNN, которая вычисляет соответствующие главные компоненты. С выходов RNN данные поступают на многослойные персептроны, которые определяют тип атаки. Арбитр принимает окончательное решение. Его структура определяется, как и в предыдущем варианте.

Кроме того, возможен вариант представленный на рис. 4, который является модификацией варианта 3. Отличительной особенностью этой нейросетевой структуры является общий для всех RNN модуль MLP. Он и производит основные вычисления, связанные с распознаванием входного вектора, одновременно используя всю информацию предоставленную рециркуляционными нейронными сетями.

Рассмотренные в данном разделе архитектурные решения систем обнаружения атак базируются на различной компиляции рециркуляционных и многослойных нейронных сетей.

3. ПРОЕКТИРОВАНИЕ НЕЙРОННЫХ СЕТЕЙ

Рассмотрим линейную рециркуляционную нейронную сеть (рис. 5). Она осуществляет сжатие 41-размерного входного вектора в 12-размерный выходной вектор. Количество главных компонент определялось экспериментальным путем исходя из достижения приемлемой точности без существенной потери информативности. Эксперименты показали, что существует некоторое оптимальное число главных компонент, дальнейшее увеличение которых не приводит к повышению качества распознавания.

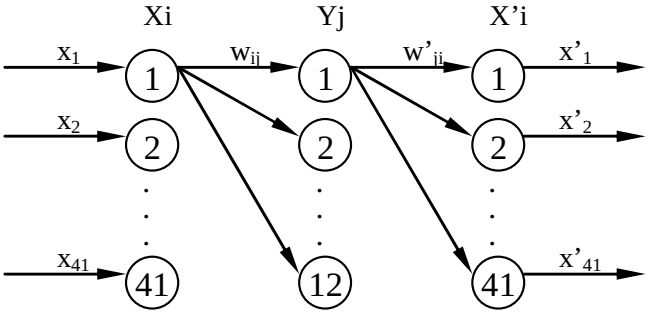
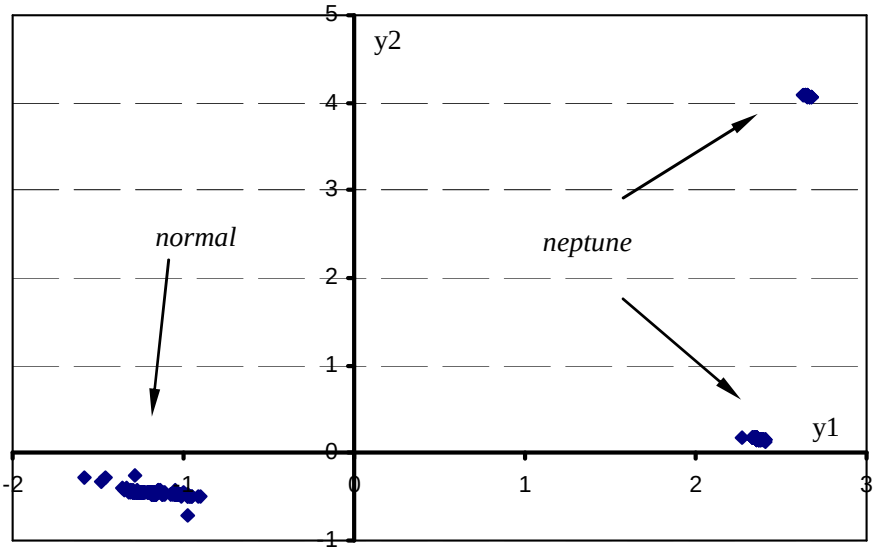


Рис. 5. Архитектура RNN



Сервис **auth**

normal	220
neptune	108

Рис. 6. Данные после обработки RNN на примере сервиса auth.

Обучение RNN производилось в соответствии с правилом Ойя [3]:

$$w'_{ji}(t+1) = w'_{ji}(t) + \alpha \cdot y_j \cdot (x_i - \overline{x_i}),$$

где w'_{ji} - весовой коэффициент между j-ым нейроном скрытого слоя и i-ым нейроном выходного слоя.

Перед подачей данных на вход RNN проводилась их предварительная обработка:

$$x_i^k = \frac{x_i^k - \mu(x_i)}{\sigma(x_i^k)},$$

где $\mu(x_i) = \frac{1}{L}\sum_{k=1}^{L} x_i^k$,

$$\sigma(x_i^k) = \frac{1}{L}\sum_{k=1}^{L}(x_i^k - \mu(x_i))^2.$$

Здесь L – размерность обучающей выборки.

Для обучения RNN использовались данные из базы KDD-99. Желаемая суммарная среднеквадратичная ошибка – 0,01. Количество повторений цикла обучения составляло 1000. После обучения сети она может преобразовывать входное пространство образов в главные компоненты.

Рассмотрим отображение входного пространства образов для нормального состояния и атаки (тип атаки neptune) на плоскость двух первых главных компонент (рис. 6).

Из рисунка видно, что данные, соответствующие одному классу атаки могут концентрироваться в нескольких областях. Это затрудняет классификацию атак при использовании RNN. Для устранения этого недостатка можно применить нелинейную RNN, что будет рассмотрено в дальнейших работах.

Как уже отмечалось, многослойный персептрон предназначен для классификации атак на основе главных компонент (рис. 7).

Количество нейронов выходного слоя варьируется в зависимости от определения типа или класса атаки. Для обучения использовался алгоритм обратного распространения ошибки. Сеть обучалась до суммарной квадратичной ошибки равной 0,01.

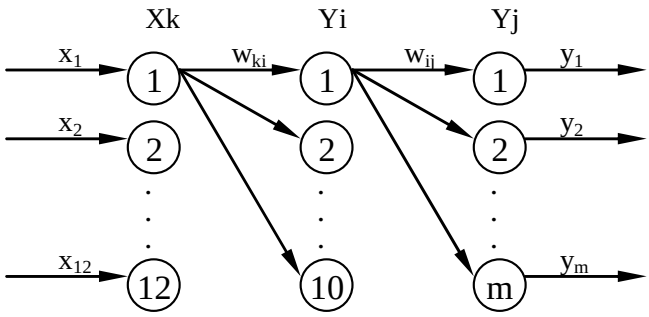


Рис. 7. Архитектура MLP с одним скрытым слоем

После обучения рассмотренных выше нейронных сетей они объединялись в единую систему обнаружения атак.

4. ЭКСПЕРИМЕНТЫ

В процессе обучения и тестирования системы использовалась 10% выборка данных из базы KDD-99. Эксперименты проводились для каждой службы отдельно. Обучающие выборки содержали около 20% записей по каждой службе. После обучения на сеть подавался весь набор имеющихся записей, и собиралась статистика обнаружения и распознавания атак.

Рассмотрим функционирование системы на примере модели 1 (см. раздел 2). Результаты тестирования в режиме распознавания класса атаки для некоторых служб приведены в таблице 1. Сводные данные по почти 30 службам приведены в таблице 2.

Таблица 2 позволяет оценить эффективность предложенного алгоритма при решении задач классификации атак. Наилучший результат был достигнут для атак класса DoS и Probe (почти однозначная распознаваемость). Несколько хуже определяются U2R и R2L, соответственно 83,7% и 89,4%. Кроме того, существует процент ложных срабатываний системы.

Далее приведен результат тестирования в режиме распознавания типа атаки, отдельно для случая с 23 выходными нейронами сети MLP (все типы атак + нормальное состояние) и для случая с их динамически настраивающимся количеством. Во втором варианте в процессе обучения подсчитывается, сколько состояний сети присутствует в обучающей выборке, и на основании полученной информации принимается решение о количестве соответствующих нейронных элементов выходного слоя.

Таблица 1. Результаты тестирования в режиме классификации атак

служба	normal		DoS			U2R		
	кол.	**распознано**	**кол.**	**обнаружено**	**распознано**	**кол.**	**обнаружено**	**распознано**
auth	220	220(100%)	108	108(100%)	108(100%)			
domain	3	3(100%)	112	112(100%)	112(100%)			
eco_I	389	387(99,5%)						
ecr_I	345	327(94,8%)	281049	281031 (100%)	281031 (100%)			
finger	468	456(97,4%)	197	189(95,9%)	85(45,0%)			
ftp	373	359(96,2%)	104	104(100%)	104(100%)	3	3(100%)	3(100%)
ftp_ data	3798	3752(98.8%)	170	168(98,8%)	26(15,5%)	12	12(100%)	11 (91,7%)
http	61885	61787(99,8%)						
IRC	42	41(97,6%)						
pop_3	79	79(100%)	118	118(100%)	118(100%)	34	26(76,5%)	26(100%)
smtp	9598	9472(98,7%)	120	120(100%)	120(100%)			
telnet	219	204(93,2%)	198	198(100%)	198(100%)	34	26(76,5%)	26(100%)

Таблица 1. Результаты тестирования в режиме классификации атак (продолжение)

служба	R2L			Probe		
	кол.	**обнаружено**	**распознано**	**кол.**	**обнаружено**	**распознано**
auth						
domain				1	1(100%)	1(100%)
eco_I				1253	1251(99,8%)	1251(100%)
ecr_I				6	0(0,0%)	0(0,0%)
finger				5	5(100%)	4(80,0%)
ftp	313	245(78,3%)	244(99,6%)	5	5(100%)	5(100%)
ftp_ data	733	683(93,2%)	595(87,1%)	8	8(100%)	7(87,5%)
http	4	4(100%)	4(100%)	8	8(100%)	8(100%)
IRC				1	1(100%)	1(100%)
pop_3				5	5(100%)	5(100%)
smtp				5	5(100%)	3(60,0%)
telnet	57	56(98,2%)	53(94,6%)	5	5(100%)	5(100%)

Таблица 2. Статистика тестирования модели 1 в режиме классификации атак (около 30 сервисов)

класс	**всего**	**обнаружено**	**распознано**
DoS	286369	286334(99,9%)	286087(99,9%)
U2R	49	41(83,7%)	40(97,6%)
R2L	1119	1000(89,4%)	906(90,6%)
Probe	1320	1312(99,4%)	1308(99,7%)
нормальное состояние			
normal	83281	---	82943(99,6%)

Таблица 3. Статистика тестирования в режиме определения типа атаки (настраиваемое число выходных нейронных элементов)

служба	**определенные атаки**	**ложное срабатывание**	**распознанные атаки**
auth	108(100%)	0	108(100%)
domain	113(100%)	0	113(100%)
eco_I	1252(99,9%)	7(1,8%)	1238(98,9%)
ecr_I	281033(99,9%)	12(3,4%)	281033(100%)
finger	202(100%)	11(2,3%)	200(99,0%)
ftp	283(66,5%)	14(3,8%)	283(100%)
ftp_data	864(93,7%)	44(1,2%)	777(89,9%)
http	2399(99,7%)	96(0,16%)	2396(99,9%)
IRC	1(100%)	1(2,38%)	1(100%)
pop_3	123(100%)	0	123(100%)
smtp	123(97,7%)	44(0,4%)	121(98,4%)
telnet	284(96,6%)	16(7,31%)	280(98,6%)

Таблица 4. Статистика тестирования в режиме определения типа атак (число выходных нейронов равняется 23)

служба	определенные атаки	ложное срабатывание	распознанные атаки
auth	108(100%)	0	108(100%)
domain	113(100%)	0	113(100%)
eco_I	1252(99,9%)	0	1239(99,0%)
ecr_I	281034(99,9%)	13(3,77%)	281034(100%)
finger	186(92,1%)	10(2,14%)	185(99,5%)
ftp	418(98,3%)	26(6,97%)	418(100%)
ftp_data	856(92,7%)	31(0,82%)	636(74,3%)
http	2400(99,7%)	96(0,16%)	2400(100%)
IRC	1(100%)	1(2,38%)	1(100%)
pop_3	123(100%)	0	123(100%)
smtp	122(97,6%)	35(0,36%)	119(97,5%)
telnet	284(96,6%)	15(6,85%)	272(95,7%)

Таблица 5. Статистика тестирования модели 4 в режиме классификации атак (около 30 сервисов)

класс	всего	обнаружено	распознано
DoS	286369	286369(100%)	286295(99,9%)
U2R	49	33(67,3%)	32(97,0%)
R2L	1119	442(39,5%)	427(96,6%)
Prode	1320	1311(99,3%)	1288(98,2%)
нормальное состояние			
normal	83281	---	77673(93,2%)

Сравнение результатов опытов с разным количеством выходных нейронных элементов показало, что полученные данные практически идентичны (см. таблица 3 и таблица 4).

Оценим эффективность модели 1 в сравнении с моделью 4 (см. таблица 2 и таблица 5). В нашем эксперименте параметры входного вектора делились на три группы - те, что принимают целочисленные значения; ключи 0/1; параметры, величины которых лежат в диапазоне от 0 до 1. Далее каждая группа подавалась на обработку соответствующей RNN. Расчет был сделан на улучшение качества обучения за счет того, что каждая RNN в этом случае обрабатывает однородные по структуре данные. Особенностью модели 4 является ее пониженная чувствительность к атакам класса U2R и R2L. В то же время эта модель может успешно применяться для распознавания наиболее широко представленных в базе KDD-99 атак класса DoS. Еще одним преимуществом модели 4 можно считать скорость ее обучения. За счет уменьшения количества связей в модуле вычисления главных компонент снижается нагрузка на системные ресурсы в процессе пересчета сети.

5. ЗАКЛЮЧЕНИЕ

В работе рассмотрены различные подходы к построению систем обнаружения атак, которые базируются на нейросетевых технологиях. Путем комбинирования двух различных нейронных сетей, а именно RNN и MLP, можно идентифицировать и распознавать атаки на компьютерные сети с достаточно высокой степенью точности. В качестве базы данных для тестирования предложенных методов использовалась база KDD-99. Основными преимуществами использования подходов, основанных на нейронных сетях, является способность адаптироваться к динамическим условиям и быстрота функционирования, что особенно важно при работе системы в режиме реального времени.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. 1999 KDD Cup Competition. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
2. Головко В.А. Нейронные сети: обучение, организация и применение. Кн. 4: Учеб. пособие для вузов / Общая ред. А.И. Галушкина. – М.: ИПРЖР, 2001. – 256 с.
3. Hyvaerinen A., Oja E. Independent component analysis: algorithms and applications // Neural Networks, №13, 2000, - P. 411-430.

УДК 681.3

Горбашко Л.А.

МЕТОД СКРЫТИЯ ИЗОБРАЖЕНИЙ С ПРИМЕНЕНИЕМ ВЕКТОРНОГО КВАНТОВАНИЯ

ВВЕДЕНИЕ

Задача защиты информации от несанкционированного доступа приобретает все большую актуальность в современном мире. Развитие информационных технологий дало новый толчок для развития компьютерной стеганографии - скрытую передачу данных в маскирующем сигнале. Сообщения встраивают в цифровые данные, имеющие аналоговую природу (речь, аудиозаписи, изображения, видео).

Для скрытой передачи информации выбирается контейнер, которым чаще всего служит графический файл. В него

***Горбашко Лариса Ашотовна**, ст. преподаватель каф. интеллектуальных информационных технологий Брестского государственного технического университета.*
Беларусь, БрГТУ, 224017, Беларусь, г. Брест, ул. Московская, 267, e-mail: lagorbashko@bstu.by.