ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 4(22) / 2016

Журнал «Вестник УрФО. Безопасность в информационной сфере» включен в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство ПИ № ФС77-65765 от 20.05.2016

Издатель: **ООО «Южно-Уральский юридический вестник»**

Адрес редакции и издателя: Россия, 454080, г. Челябинск, пр. Ленина, д. 76.
Тел./факс (351) 267-97-01.

Электронная версия журнала в Интернете:
www.info-secur.ru,
e-mail: urvest@mail.ru

16+

В НОМЕРЕ

ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

МАТЕМАТИЧЕСКИЕ МЕТОДЫ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОРГАНИЗАЦИОННАЯ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

ПРАКТИЧЕСКИЙ АСПЕКТ

TECHNICAL MEANS AND METHODS OF INFORMATION PROTECTION

COMPUTER SECURITY

MATHEMATICAL METHODS IN INFORMATION SECURITY

ORGANIZATIONAL AND ORGANIZATIONAL - TECHNICAL PROTECTION OF INFORMATION

LEGAL REGULATION OF INFORMATION SECURITY

THE PRACTICAL ASPECT

УДК 621.391.2 + 004.056 + 004.4.056 Вестник УрФО № 4(22) / 2016, с. 4–10

Носов Л. С., Зудин В. С.

МОДЕЛЬ ОЦЕНКИ ЗАЩИЩЕННОСТИ ПО КАНАЛУ ПЭМИН ПОСРЕДСТВОМ ОПРЕДЕЛЕНИЯ СТЕПЕНИ РАСПОЗНАВАНИЯ СИГНАЛА

В работе приведена модель оценки защищенности по каналу ПЭМИН. В качестве оценки предлагается степень разборчивости сигнала ПЭМИН, методика определения которой приведена в работе. Определены параметры измерительного оборудования, при котором данная методика применима. Разработано программное обеспечение для оценки разборчивости, которое протестировано с использованием спектроанализатора Rohde & Schwarz FS300.

Ключевые слова: *ПЭМИН, аналоговый сигнал, объект информатизации, видеодисплейный монитор, электромагнитные излучения.*

Nosov L. S., Zudin V. S.

TEMPEST SECURITY ASSESSMENT MODEL BY DETERMINING THE DEGREE OF SIGNAL DETECTION

The TEMPEST security assessment model is observed in the work. As the degree of intelligibility proposed assessment TEMPEST signal, the method defined in the work. The parameters of the measuring equipment are obtained, in which the technique is applicable. Software for the determining the degree of signal has been developed, which was tested using a spectrum analyzer Rohde & Schwarz FS300.

Keywords: *TEMPEST, analog signal, informatization object, video display monitor, electromagnetic radiation.*

Одни из первых известных предположений о возможности извлечения информации из побочных излучений были сделаны в работах Герберта Ядли (Herbert Yardley) ещё в начале XX века. Военные секретные исследования ПЭМИН ведутся, по крайней мере, с начала 60-х годов[1] (некоторые источники говорят о конце 40-х - начале 50-х годов[2]). Первое упоминание побочных электромагнитных излучений, как риска компьютерной безопасности, было сделано в 1967 г. Одно из первых детальных описаний появилось в 1983 г. Широкую огласку проблема ПЭМИН получила в 1985 г. после статьи голландского инженера Вима ван Эйка (Wim van Eck) «Электромагнитное излучение видеодисплейных модулей: Риск перехвата?». Особенно сильный эффект произвела, сделанная им в этом же году на выставке Securecom-85, демонстрация перехвата излучений монитора с использованием слегка доработанного телевизионного приемника. С этого момента, перехват ПЭМИН перестал восприниматься как нечто дорогостоящее и доступное только государственным спецслужбам, и у частных организаций появился повод рассматривать этот риск как актуальный и требующий оценки[1].

Для оценки защищённости объектов информатизации от утечки информации по каналу ПЭМИН используются специальные методики. На этом этапе возникает проблема: все наиболее известные методики являются информацией ограниченного доступа. По этой причине усилия в этой работе было решено направить на разработку и программную реализацию открытой методики оценки защищенности информации от утечки по каналу ПЭМИН. Вопрос является довольно объёмным, поэтому исследование будет ограниченно излучениями монитора, использующего аналоговое подключение к компьютеру.

Все наиболее известные методики оценки защищенности информации от утечки по каналу ПЭМИН являются информацией ограниченного доступа. Это накладывает ряд ограничений на организации, желающие самостоятельно проводить оценки собственного оборудования, не прибегая к информации ограниченного доступа.

Цель настоящей работы – разработка и программная реализация открытой методики оценки защищённости информации от утечки по каналу ПЭМИН на примере излучений монитора.

Компонентный видеоинтерфейс VGA, используемый для подключения мониторов, был выпущен фирмой IBM в 1987 г. видеосигнал для такого интерфейса рассчитан на работу с ЭЛТ-мониторами, что и определяет его особенности. Во-первых, ЭЛТ-мониторы используют строчную развёртку, поэтому изображение в сигнале кодируется построчно. Во-вторых, сигнал подаётся на катод электронной пушки, поэтому он характеризуется отрицательной полярностью, т.е. белый пиксель соответствует уровню 0 В, а чёрный – уровню $-U_{\max}$[3,4,5]. Подробный анализ сигнала VGA можно найти в работах [6,7]. Помимо этого, видеосигнал обладает тремя частотными характеристиками[1]. За инструкциями по получению характеристик видеосигнала следует обратиться к документации к используемой видеокарте. Иногда информация может обнаруживаться в конфигурационных файлах системы. Кроме того, существуют стандарты VESA, определяющие продолжительности зон (их ещё называют тайминги, от англ. timings) в зависимости от разрешения и какой-нибудь частотной характеристики (некоторые из этих стандартов свободно доступны, например работа[8], по другим есть информация в косвенных источниках, например в работе[7].

Расчёт характеристик видеосигнала по разрешению и частоте обновления экрана был реализован в программе «Калькулятор таймингов VESA». Калькулятор использует формулы VESA Generalized Timing Formula (GTF)[7]. Цветные мониторы отличаются тем, что вместо одного, к ним идут сразу три канала, каждый из которых кодирует яркость одного из базовых цветов: красного, синего или зелёного. Так как эти каналы передают и излучают синхронно, отделить один цветовой канал от другого, при перехвате ПЭМИН невозможно, поэтому, с точки зрения ПЭМИН, цветной монитор не отличается от чёрно-белого[3,4,5].

Тестовый сигнал должен моделировать ситуацию, в которой оказывается злоумышленник при перехвате информации по каналу ПЭМИН. Рассмотрим некоторые особенности, возникающие при таком перехвате. Чтобы кабель излучал, в нём должен протекать переменный ток. Это значит, что злоумышленник будет наблюдать сигнал в эфире только тогда, когда в кабеле меняется уровень напряжения, т.е. когда в изображении возникает цветовой переход. В связи с этим, а также с тем,

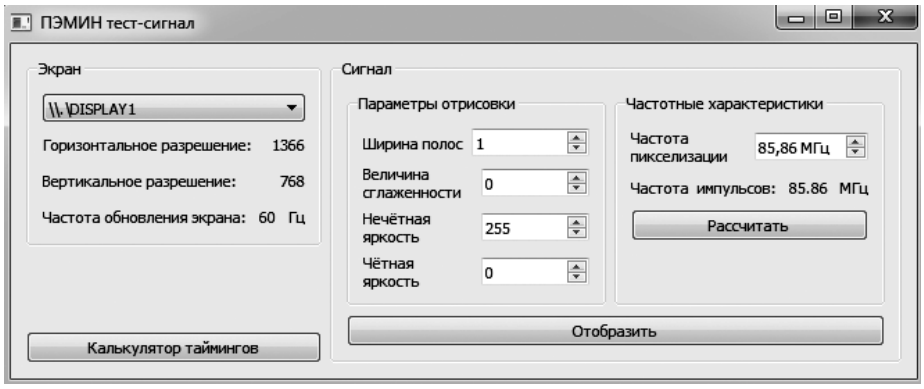

Рис. 1. Интерфейс программы «ПЭМИН тест-сигнал»

что через ПЭМИН неразличимы цветовые компоненты, перехват, в первую очередь, рассчитан на двухцветные изображения (чёрный текст на белом фоне – наиболее распространённый вид такого изображения)[1]. Перехваченное изображение, в этом случае, содержит контуры исходного.

Тогда качество распознавания изображения можно определять по точности определения границ цветовых переходов на изображении. Очевидно, что, благодаря построчной развёртке, имеют значение только горизонтальные переходы, поэтому, тестовый сигнал может представлять собой чередование вертикальных полос двух цветов. Для такого сигнала можно определить несколько параметров:

- Ширина полосы в пикселях;
- Разность яркости соседних полос;
- Сглаженность перехода в пикселях.

Описанный тестовый сигнал реализован в программе «ПЭМИН тест-сигнал». Интерфейс программы представлен на рис. 1.

Раздел «Экран» определяет монитор, на котором следует отобразить тестовый сигнал. Раздел «Параметры отрисовки» определяет параметры тестового сигнала. Раздел «Частотные характеристики» является вспомогательным: он позволяет рассчитать частоту цветовых переходов заданного тестового сигнала по известной частоте пикселизации. Кнопка «Калькулятор таймингов» вызывает окно, эквивалентное программе «Калькулятор таймингов VESA» (см. выше), в котором параметры видеорежима установлены в соответствии с выбранным в разделе «Экран» монитором. Частота пикселизации, рассчитанная калькулятором таймингов, автоматически установится в разделе «Частотные характеристики».

Порядок и особенности выполнения измерений зависят от применяемого оборудования, поэтому эту задачу имеет смысл отделить от остальной части оценки. В рамках этой работы планировалось использовать спектроанализатор Rohde & Schwarz FS300. Он поддерживает удалённое управление с компьютера. Порядок удалённой работы со спектроанализатором описан в руководствах к нему [9,10].

Инструмент для выполнения измерений был реализован в виде программы «Измеритель: R&S серии FS3xx». Интерфейс программы представлен на рис. 2.

Во время тестирования измерителя, выяснилось, что достижимой частоты дискретизации спектроанализатора Rohde & Schwarz FS300 недостаточно для проведения тестов, т.к. фактически теряются практически все горизонтальные составляющие. Например, на рис. 3 изображён тестовый сигнал, и соответствующее ему перехваченное изображение. Как можно видеть, горизонтальные переходы в пределах строки практически отсутствуют.

Чтобы таких проблем не возникало, при выборе измерителя следует руководствоваться следующим правилом: если сигнал имеет частоту пикселизации f_p, и планируется оценивать распознаваемость объектов, с горизонтальными размерами не менее w пикселей (ширина полосы в тестовом сигнале из раздела 3.2 не менее w), минимальная частота дискретизации прибора вычисляется по следующей формуле:

$$f_d = \frac{2 f_p}{w} \qquad (1)$$

В данной работе, доступа к измерителю с необходимыми характеристиками получить не удалось, поэтому дальнейшую разработку придётся продолжать без проведения тестов. Наиболее простой и, возможно, эффективный способ выделения кадра – это ручное

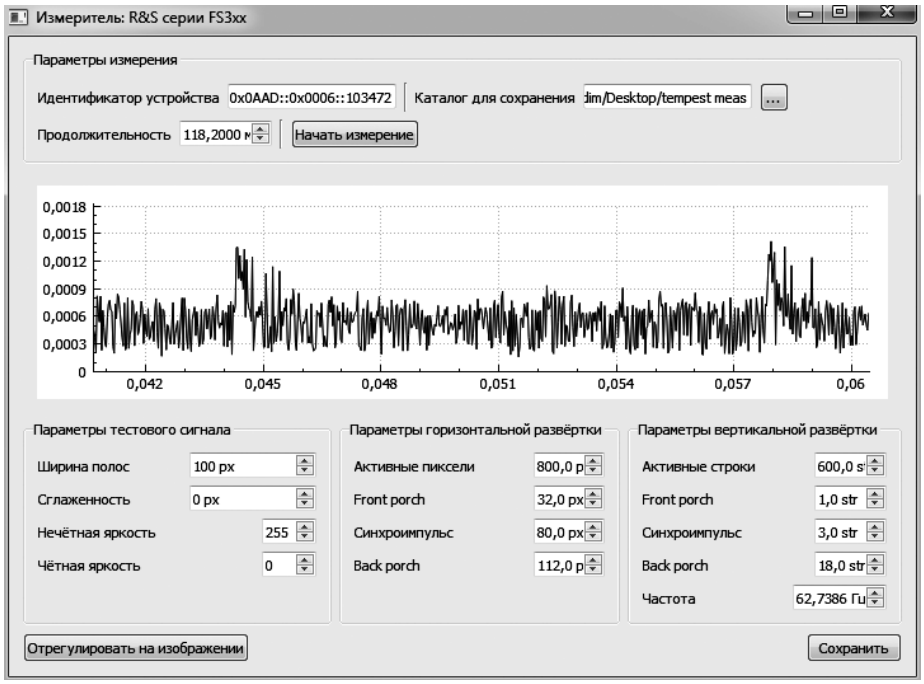

Рис. 2. Интерфейс программы « Измеритель: R&S серии FS3xx»

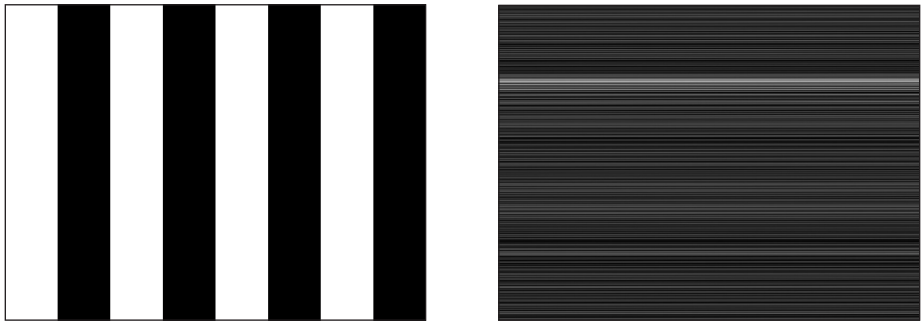

Рис. 3. Пример тестового сигнала (слева) и соответствующее ему перехваченное изображение (справа).

выделение оператором. Однако при обработке большого количества измерений такой метод создаёт большую нагрузку на человека. В этом разделе предпринята попытка предложить метод автоматического выделения кадра.

Зная параметры исследуемого монитора, параметры тестового сигнала и способ его образования, можно попытаться предсказать форму сигнала ПЭМИН. Для тестового сигнала, описанного выше, ПЭМИН должен представлять собой последовательность коротких импульсов. Ниже дано описание правил определения положения этих импульсов.

Пусть определены следующие характеристики сигнала: T_{pulse} – период следования цветовых переходов тестового сигнала; T_h – период горизонтальной развёртки; t_{h_active} – продолжительность горизонтальной «активной» области; t_{h_fp} – время начала строкового «front porch» от начала строки; t_{h_sync} – время начала строкового синхроимпульса от начала строки; t_{h_bp} – время начала строкового «back porch» от начала строки; T_v – период вертикальной развёртки; t_{v_active} – продолжительность вертикальной «активной» области; t_{v_fp} – время начала вертикального «front porch» от начала кадра; t_{v_sync} – время начала вертикального синхроимпульса от начала кадра; t_{v_bp} – время начала вертикального «back porch» от начала кадра; b_1 – нечётная яркость; b_2 – чётная яркость. Яркость последней полосы в строке b_{last} можно определить следующим образом: $b_{last} = b_1$, если $\left[\frac{T_h}{T_{pulse}}\right]$ – нечётное, $b_{last} = b_2$, если $\left[\frac{T_h}{T_{pulse}}\right]$ – чётное. Здесь […] – взятие целой части.

Для некоторого момента времени t, время от начала кадра t_v, время от начала строки t_h и время от последнего цветового перехода t_{pulse} определяются следующим образом:

$$t_v = t - \left[\frac{t}{T_v}\right] \times T_v, \; t_h = t_v - \left[\frac{t}{T_h}\right] \times T_h,$$
$$t_{pulse} = t_h - \left[\frac{t}{T_{pulse}}\right] \times T_{pulse} \tag{2}$$

Если задана ширина импульса w_{pulse}, то t принадлежит импульсу образцового сигнала, если оно удовлетворяет следующему условию:

$$\begin{aligned}
&\left(\left(t_v < w_{pulse}/2\right) \wedge \left(b_1 > 0\right)\right) \vee \left(\left|t_v - t_{v_sync}\right| < w_{pulse}/2\right) \vee \\
&\left(\left(t_v < w_{pulse}/2\right) \wedge \left(b_1 > 0\right)\right) \vee \left(\left|t_v - t_{v_bp}\right| < w_{pulse}/2\right) \vee \\
&\left(\left(T_v - t_v < w_{pulse}/2\right) \wedge \left(b_1 > 0\right)\right) \vee \left(\left(t_h < w_{pulse}/2\right) \wedge \left(b_1 > 0\right) \wedge \left(t_v > t_{v_fp}\right)\right) \vee \\
&\left(\left(\left|t_h - t_{h_fp}\right| < w_{pulse}/2\right) \wedge \left(b_{last} > 0\right) \wedge \left(t_v > t_{v_fp}\right)\right) \vee \\
&\left(\left(\left|t_h - t_{h_sync}\right| < w_{pulse}/2\right) \wedge \left(\left(t_v < t_{v_sync}\right) \vee \left(t_v > t_{v_bp}\right)\right)\right) \vee \\
&\left(\left(\left|t_h - t_{h_bp}\right| < w_{pulse}/2\right) \wedge \left(\left(t_v < t_{v_sync}\right) \vee \left(t_v > t_{v_bp}\right)\right)\right) \vee \\
&\left(\left(T_h - t_h < w_{pulse}/2\right) \wedge \left(b_1 > 0\right) \wedge \left(t_v < t_{v_fp} - w_{pulse}/2\right)\right) \vee \\
&\left(\left(t_{pulse} < w_{pulse}/2\right) \wedge \left(t_h > w_{pulse}/2\right) \wedge \left(t_h < t_{h_fp} - w_{pulse}/2\right)\right) \vee \\
&\left(\left(T_{pulse} - t_{pulse} < w_{pulse}/2\right) \wedge \left(t_h > w_{pulse}/2\right) \wedge \left(t_h < t_{h_fp} - w_{pulse}/2\right)\right)
\end{aligned} \tag{3}$$

здесь: $\wedge$ – логическое «И», $\vee$ – логическое «ИЛИ». Используя условия из формулы (3), можно сгенерировать образцовый сигнал в любом временном диапазоне.

Так как продолжительность кадра T_v известна, необходимо только определить смещение кадра в исследуемом сигнале. Для этого можно воспользоваться способом определения смещения между похожими сигналами по максимуму функции корреляции [12]. Порядок операций следующий:

1) сгенерировать образцовый сигнал на временном диапазоне $[0, T_v)$;

2) на промежутке $[0; T_v)$ рассчитать значения функции корреляции между исследуемым и образцовым сигналами;

3) смещение принять равным положению максимума функции корреляции.

Как уже было указано выше, качество распознавания изображения можно определять по точности определения границ цветовых переходов на изображении. Можно выделить два вида ошибок: потеря цветового перехода и обнаружение ложного цветового перехода. Соответственно, можно определить две метрики информативности ПЭМИН: процент потерянных цветовых переходов и процент ложных цветовых переходов (относительно ожидаемого числа цветовых переходов). Ниже предложен способ вычисления этих метрик. Расчёт описанных метрик был реализован в программе «Оценка ПЭМИН».

Первое, что необходимо определить, это ожидаемое расположение цветовых переходов. Определим яркость последней полосы в строке b_{last}. Для некоторого момента времени t, в соответствии с формулой (2), определим время от начала кадра t_v, время от начала строки t_h и время от последнего цветового перехода t_{pulse}. Тогда t является ожидаемым положением цветового перехода, если оно удовлетворяет следующему условию:

$$\begin{aligned}
&\left(\left(t_h = 0\right) \wedge \left(b_1 > 0\right) \wedge \left(t_v < t_{v_active}\right)\right) \vee \left(\left(t_h = t_{h_active}\right) \wedge \left(b_{last} > 0\right) \wedge \left(t_v < t_{v_active}\right)\right) \vee \\
&\left(\left(t_h = T_h\right) \wedge \left(b_1 > 0\right) \wedge \left(t_v < t_{v_active}\right)\right) \vee \left(\left(t_{pulse} = 0\right) \wedge \left(t_v < t_{v_active}\right) \wedge \left(t_h > 0\right)\right) \vee \\
&\left(\left(t_{pulse} = T_{pulse}\right) \wedge \left(t_v < t_{v_active}\right) \wedge \left(t_h < t_{h_active}\right)\right)
\end{aligned} \tag{4}$$

Используя условия из формулы (4), можно сгенерировать массив ожидаемых расположений цветовых переходов в любом временном диапазоне. Следующее, что необходимо определить – это расположение цветовых переходов в исследуемом сигнале. Эта задача сводится к поиску и определению положения пиков. К сожалению, из-за наличия шумов, простой поиск точек локального максимума может не дать нужного результата. В этой работе предлагается другой способ поиска пиков в сигнале:

1) Задать размер окна w (в секундах) и значение порога для углового коэффициента $k_{\min}$. На интуитивном уровне, w определяет ширину пика, а $k_{\min}$, определяет минимальную скорость роста сигнала до точки пика и минимальную скорость падения сигнала после точки пика.

2) Для каждой точки сигнала t выделить два диапазона: $\left[t-\frac{w}{2};t\right]$ и $\left[t;t+\frac{w}{2}\right]$.

3) Используя метод наименьших квадратов [10], аппроксимировать оба диапазона линейной зависимостью. Обозначим полученные угловые коэффициенты как k_1, для диапазона $\left[t-\frac{w}{2};t\right]$ и k_2, для диапазона $\left[t;t+\frac{w}{2}\right]$.

4) Рассматриваемая точка t будет считаться точкой пика, если $k_1 > k_{\min}$ и $k_2 < -k_{\min}$.

5) Если, согласно предыдущему правилу, к точке пика были отнесены несколько соседних точек сигнала, то их следует заменить одной, равной их среднему.

Порядок вычисления процента потерянных цветовых переходов $p_{пот}$ и процента ложных цветовых переходов $p_{лож}$ можно определить следующим образом:

1) Задать пороговое значение $\Delta_{\max}$, задающее максимально допустимое отклонение реального пика от его ожидаемого положения.

2) Создать счётчики числа ложных импульсов $n_{лож}$ и числа потерянных импульсов $n_{пот}$. Установить их равными нулю.

3) Сгенерировать массив ожидаемых расположений цветовых переходов (образцовый массив) на промежутке времени, соответствующему исследуемому сигналу. Записать его длину в переменную n.

4) Сгенерировать массив расположений цветовых переходов в исследуемом сигнале (исследуемый массив).

5) Создать вспомогательный массив.

6) Создать переменную для хранения текущего положения в исследуемом массиве и установить её равной -1.

7) Для каждого значения в образцовом массиве выполнить следующие действия:

- найти ближайший элемент в исследуемом массиве;
- рассчитать точность, как разницу между значением образцового массива и значением ближайшего элемента исследуемого массива;

рассчитать смещение s в исследуемом массиве, как разницу между индексом найденного элемента исследуемого массива и текущим положением в исследуемом массиве;

- если $s = 0$, то увеличить $n_{пот}$ на 1, и, если последний элемент вспомогательного массива больше точности, установить его равным точности;
- если $s = 1$, то добавить значение точности во вспомогательный массив;
- если $s > 1$, увеличить $n_{лож}$ на $s-1$ и добавить значение точности во вспомогательный массив.

8) Для каждого элемента во вспомогательном массиве, если значение элемента больше $\Delta_{\max}$, увеличить счётчики $n_{лож}$ и $n_{пот}$ на 1.

9) Рассчитать процент потерянных цветовых переходов по следующей формуле: $p_{пот} = \frac{n_{пот}}{n} \times 100\%$.

10) Рассчитать процент ложных цветовых переходов по следующей формуле: $p_{лож} = \frac{n_{лож}}{n} \times 100\%$.

В ходе настоящей работы разработаны метрики информативности ПЭМИН аналогового видеосигнала и составлена методика оценки защищённости монитора от утечки информации по каналу ПЭМИН и выполнена программная реализация полученной методику оценки защищённости.

Примечания

1. Kuhn M. G., Anderson R. J. Soft Tempest: Hidden data transmission using electromagnetic emanations. – United Kingdom.: University of Cambridge, 1998. – 19 p.

2. Мотуз О. В. Побочные электромагнитные излучения: моменты истории // Сайт проекта Агентура. Ru. – URL: http://www.agentura.ru/culture007/history/tempest/ (дата обращения: 17.11.2016).

3. Кондратьев А. В. К вопросу оценки ПЭМИН цифровых сигналов. TFT мониторы. Часть 1 // Официальный сайт группы компаний МАСКОМ. – URL: http://www.mascom.ru/library/statyi/k-voprosu-otsenki-pemin-tsifrovykh-signalov-tft-monitory.php (дата обращения: 17.11.2016).

4. Кондратьев А. В. К вопросу оценки ПЭМИН цифровых сигналов. TFT мониторы. Часть 2 // Официальный сайт группы компаний МАСКОМ. – URL: http://www.mascom.ru/library/statyi/k-voprosu-otsenki-pemin-tsifrovykh-signalov-tft-monitory-chast-2.php (дата обращения: 17.11.2016).

5. Кондратьев А. В. К вопросу оценки ПЭМИН цифровых сигналов. TFT мониторы. Часть 3 // Официальный сайт группы компаний МАСКОМ. – URL: http://www.mascom.ru/library/statyi/k-voprosu-otsenki-pemin-tsifrovykh-signalov-tft-monitory-chast-3.php (дата обращения: 17.11.2016).

6. VGA Hardware // Wiki проекта OS Project. – URL: http://wiki.osdev.org/VGA_Hardware (дата обращения: 17.11.2016).

7. Video signals and timing // Wiki проекта OS Project: URL: http://wiki.osdev.org/Video_Signals_And_Timing (дата обращения: 17.11.2016).

8. VESA Display Monitor Timing Standard «VESA and Industry Standards and Guidelines for Computer Display Monitor Timing (DMT)» // Video Electronics Standards Association. – 2007.

9. Remote Control Manual Series300 Spectrum Analyzer. VXI Plug & Play Style Instrument Driver. – Germany.: ROHDE & SCHWARZ GmbH & Co. KG, 2006. – 185 p.

10. Rohde & Schwarz Smart Instruments Family300 Basic Programming Guide. – Germany.: ROHDE & SCHWARZ GmbH & Co. KG, 2007. – 23 p.

НОСОВ Леонид Сергеевич, заведующий кафедрой информационной безопасности института точных наук и информационных технологий ФГБОУ ВО «Сыктывкарский государственный университет имени Питирима Сорокина», к.ф.-м.н., доцент. 167001, г. Сыктывкар, Октябрьский пр., д. 55. E-mail: nosov@syktsu.ru

ЗУДИН Вадим Станиславович, студент института точных наук и информационных технологий ФГБОУ ВО «Сыктывкарский государственный университет имени Питирима Сорокина». 167001, г. Сыктывкар, Октябрьский пр., д. 55. E-mail: nosov@syktsu.ru

NOSOV Leonid, Head of Department of Information Security of The Institute of Exact Sciences and Information Technology of Federal State Budget Educational Institution of Higher Education «Syktyvkar State University named after Pitirim Sorokin», Physics and Mathematics PhD, assistant professor. Bld. 55, Oktyabrsky pr, Syktyvkar, 167001. E-mail: nosov@syktsu.ru

ZUDIN Vadim, student of The Institute of Exact Sciences and Information Technology of Federal State Budget Educational Institution of Higher Education «Syktyvkar State University named after Pitirim Sorokin». Bld. 55, Oktyabrsky pr, Syktyvkar, 167001. E-mail: nosov@syktsu.ru

Вестник УрФО № 4(22) / 2016, с. 11–14

УДК 004.7.057.4 + 621.391.2 + 621.396.4

Безукладников И. И., Миронова А. А.

МЕТОДЫ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ НА СЕТЕВОМ УРОВНЕ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

В предложенной статье рассматривается метод несанкционированного доступа известный под названием «скрытые каналы». Определены такие понятия, как «скрытый канал» и «недоиспользованный ресурс». Отражены основные особенности построения «скрытых каналов» на сетевом уровне телекоммуникационных систем. Приведены примеры «скрытых каналов» на сетевом уровне модели OSI. Дано детальное описание канала с использованием модели дискретного канала связи.

Ключевые слова: *телекоммуникационные системы, несанкционированный доступ, сетевой уровень модели OSI, «скрытые каналы», недоиспользованный ресурс, параметр MTU, модель дискретного канала связи.*

Bezukladnikov I. I., Mironova A. A.

THE METHODS OF COVERT DATA TRANSMISSION ON THE NETWORK LAYER OF THE TELECOMMUNICATION SYSTEMS

In the current article such method of unauthorized access as "covert channels" are covered. The notions of "covert channels" and "half used resource" are defined. The basic features of covert channels' construction on the network layer of the telecommunicational systems are also stated in the article. The examples of "covert channels" on the network layer of the OSI model are given. The detailed description of the channel, using the model of the discrete communication channel is suggested.

Keywords: *telecommunicational systems, unauthorized access, network layer of the OSI model, "covert channels", half used resource, MTU setting, model of the discrete communication channel*

В последнее время информационные атаки на телекоммуникационные системы (ТКС) различного назначения становятся все более изощренными. Злоумышленники ищут новые, более эффективные, методы несанкционированного доступа (НСД), характеризующиеся высокой сложностью обнаружения и борьбы с ними. Поэтому, стали возникать угрозы нового поколения, которым раньше не уделялось должного внимания, так как их реализация считалась невозможной. К угрозам такого рода относится осуществление НСД посредством т.н. «скрытых каналов».

«Скрытые каналы» (СК) - методы передачи нелегальной информации незаметно для действующих средств информационной безопасности (ИБ). Принцип их функционирования основан на использовании ресурсов канала, позволяющих в процессе открытой передачи информации внести некоторые изменения, которые не повлекут за собой вред открытой передаче информации пользователя (недоиспользованный ресурс)[1]. Недоиспользованным ресурсом может служить, например, ресурс, выделенный под передачу служебной информации.

В СМИ все чаще стали появляться публикации, связанные с передачей нелегальной информации посредством СК. Однако подавляющее большинство авторов чаще описывают протоколы прикладного и транспортного уровней модели ISO/OSI для реализации СК. В настоящей статье отражены основные особенности построения СК на сетевом уровне ТКС и приведены примеры СК на данном уровне.

В общем виде для создания скрытого канала необходимо выполнить следующие основные задачи:

1. Проанализировать принцип действия и особенности технологии, используемой на соответствующем уровне легальной системы. Предложить принцип, который может быть использован для скрытого переноса информации.

2. Оценить действующую политику ИБ, и выделить ее аспекты, относящиеся к выбранному уровню, а также выделить иные действующие в системе ограничения, препятствующие реализации скрытой передачи информации при помощи предлагаемого принципа.

3. Проанализировать выполнение необходимых условий существования скрытого канала.

4. Предложить конкретную реализацию скрытого канала, использующего предлагаемый принцип передачи информации.

5. Оценить основные технические характеристики полученной реализации скрытого канала[2].

Необходимо отметить, что реализация скрытых каналов на нижних уровнях модели ISO OSI сопряжена с резким ростом числа действий злоумышленника, необходимых для реализации такого канала. Это происходит по причине того, что при реализации СК на произвольном уровне модели OSI злоумышленник пользуется функционалом нижележащих уровней открытого канала. Так, например, реализуя СК на транспортном уровне, злоумышленнику нет необходимости беспокоиться о помехоустойчивости, множественном доступе к среде, генерации маршрутов и т.д. Чем ниже уровень, используемый для СК, тем большее число этих функций должно быть реализовано злоумышленником самостоятельно[1]. По этой причине наиболее выгодным для злоумышленника является реализация СК на уровнях начиная от сетевого и выше. Пример скрытых каналов сетевого уровня в IP-потоке рассмотрен далее.

Варианты СК на сетевом уровне модели ISO OSI

Вариант 1: При передаче данных на сетевой уровень модели OSI поступает IP пакет. Размер данного пакета должен соответствовать параметру MTU (maximum transmission unit), который задается типом локальной или глобальной сети. Поскольку чаще пакет имеет размер больше максимально допустимого для передачи, он подвергается фрагментации. Так, например, сеть Ethernet имеет параметр MTU равный 1500 байт, это означает, что полезные данные IP пакета необходимо разделить на кадры. При делении пакета часто оставаться остаток (хвост), благодаря которому возникает структурная недоиспользованность информационного потока, которая может быть использована в злоумышленных целях. На рис. 1 показан пример фрагментации IP пакета в условиях сети Ethernet.

Скрытая передача информации в данном случае возможна путем заполнения на передающей стороне недоиспользованного ресурса IP-пакета с помощью определенного алфавита.

Данный пример СК по виду недоиспользованности информационного ресурса мо-

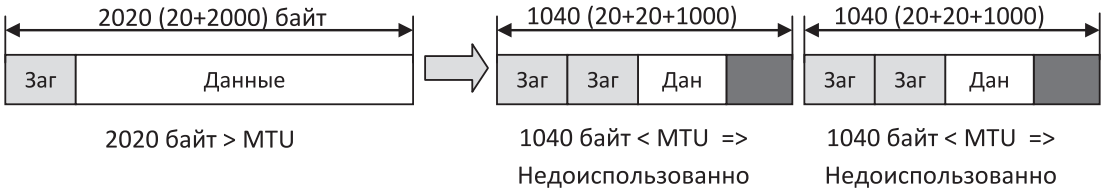

Рис. 1. Пример фрагментации IP пакета

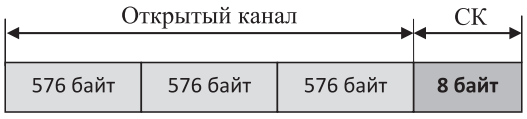

Рис. 2. Пример СК

жет быть классифицирован как недоиспользование логической структуры информационного потока.

Для детального описания канала представим его, используя модель дискретного канала связи[3]:

Участник X передает информацию участнику Y, при этом входной алфавит состоит из M символов y_i, а выходной из N символов x_i. Таким образом, в общем случае матрица канала связи содержит все переходные вероятности $P(x_i/y_i)$ и имеет вид:

$$P_{X/Y} = \begin{pmatrix} P(x_1y_1) & P(x_2y_1) & \cdots & P(x_Ny_1) \\ P(x_1y_2) & P(x_2y_2) & & P(x_Ny_2) \\ \vdots & & \ddots & \vdots \\ P(x_1y_M) & P(x_2y_M) & \cdots & P(x_Ny_M) \end{pmatrix}$$

где $P_{X/Y}$ - вероятность приема символа y_i при передаче символа x_i, от участника X к участнику Y.

В случае двоичного симметричного канала матрица примет следующий вид:

$$P_{X/Y} = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$$

где p – вероятность успешной передачи, $1\text{-}p$ – вероятность ошибки.

Например, при открытой передаче пакета показанного на рис. 2, возникает недоиспользованность. При этом заданно, что если недоиспользованность менее 8 байт, то СК не может функционировать. Следовательно, в данном случае алфавит будет иметь 2^8 символов. При этом:

$$A = B = \{a_0, a_1, \dots, a_{255}\}$$

где A – выходной алфавит, B – входной алфавит. Мощность СК в данном случае будет равна $|A|$=256 символов.

В общем случае, пропускная способность двоичного симметричного канала может быть найдена по формуле[3]:

$$C = (1-p)\log_2\big(2(1-p)\big) + p\log_2(2p)$$

В приведенном выше примере пропускная способность СК может быть найдена следующим образом:

Если пакеты имеют одинаковый размер, максимальная скорость передачи информации в СК равна: $V_{\text{СК}} = V_{\text{откр.кан.}} * 8$, где $V_{\text{откр.кан.}}$ - пакетная скорость в открытом канале;

Если пакеты имеют разный размер:

$$V_{\text{СК}} = \frac{\sum_{i=1}^{n} K_1 + K_2 + \cdots + K_n}{n}$$

$$K_n = mod\,(\frac{Q_{\text{откр.инф}}}{576})/8$$

где K_n – объем переданной информации по СК, за одно изменение состояния, $Q_{\text{откр.инф}}$ – объем открытой информации.

Вариант 2: Для структурированного информационного потока существуют случаи, когда модуляция временных интервалов между различными событиями в информационном потоке не оказывает влияния на передаваемые открытые данные[1]. Таким образом, изменение временного интервала, так же может повлечь за собой скрытую передачу данных (рис. 3).

В простейшем случае возможна передача информации по СК с использованием входного и выходного алфавита состоящего из двух символов (например, «0» и «1»):

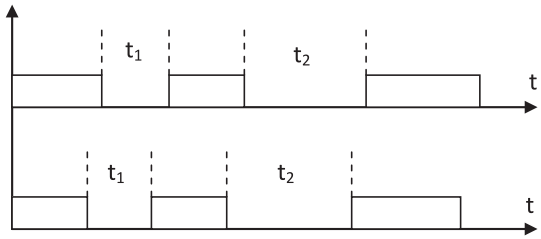

Рис. 3. Пример СК

1. передача «0», возможна при условии $0 < t_{\text{пак}} < t_1$;

2. передача «1», при условии $t_1 < t_{\text{пак}} < t_2$.

Данный вариант СК, так же может быть описан с помощью модели дискретного канала связи. Пропускная способность может быть найдена аналогично варианту 1.

Стандартные политики ИБ, составленные на основе действующего законодательства, не могут помешать работе, приведенных выше СК. Например, использование таких средств, как межсетевые экраны, антивирусные программы, датчики атак и. др. не могут создать препятствие для скрытой передачи информации данными методами.

Таким образом, проведенный анализ СК, которые могут беспрепятственно функционировать на сетевом уровне ТКС, позволяет охарактеризовать особенности отдельного класса угроз информационной безопасности. В связи с тем, что используемые в рамках функционирования СК принципы скрытой передачи информации не учитываются в большинстве политик информационной безопасности, данная проблема может считаться достаточно актуальной. Дальнейшее исследование проблемы СК предполагает нахождение способов их выявления и уничтожения, внесения соответствующих изменений в действующие требования в системе политик ИБ для совершенствования систем защиты информации ТКС.

Примечания

1. Безукладников И.И. Особенности синтеза скрытых каналов в многоуровневых системах / И. И. Безукладников, Е. Л. Кон // Системы мониторинга и управления: сборник научных трудов / Академия электротехнических наук Российской Федерации; Пермский государственный технический университет; Под ред. Е. Л. Кона .— Пермь, 2010 .— С. 230-238.

2. Безукладников И.И. Скрытые каналы в распределенных автоматизированных системах / И.И.Безукладников, Е.Л.Кон // Вестник УГАТУ, 2010, Т.14 №2. С. 245-250.

3. Гладких А. А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи / А. А. Гладких. – Ульяновск : УлГТУ, 2010. – С. 149-151.

БЕЗУКЛАДНИКОВ Игорь Игоревич, кандидат технических наук, доцент кафедры Автоматика и телемеханика Пермского национального исследовательского политехнического университета; 614990, Пермь, Комсомольский пр., 29. E-mail: fantomtk@yandex.ru.

МИРОНОВА Анна Алексеевна, студент кафедры Автоматика и телемеханика Пермского национального исследовательского политехнического университета; 614990, Пермь, Комсомольский пр., 29. E-mail: mir550@yandex.ru.

BEZUKLADNIKOV Igor' Igorevich, PhD of Technical Sciences at the Department of Automation and Telemechanics, Perm National Research Polytechnic University; 614990, 29, Komsomolsky prospect, Perm. E-mail: fantomtk@yandex.ru.

MIRONOVA Anna Alekseevna, student at the Department of Automation and Telemechanics, Perm National Research Polytechnic University, 614990, 29, Komsomolsky prospect, Perm. E-mail: mir550@yandex.ru.

УДК 004.056.53 + 658.1 : 004.056.53 Вестник УрФО № 4(22) / 2016, с. 15–20

Шабуров А. С., Журилова Е. Е.

МОДЕЛЬ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ DLP-РЕШЕНИЙ ДЛЯ ЗАЩИТЫ КОРПОРАТИВНЫХ СИСТЕМ

В данной статье проанализированыварианты оценки эффективности DLP-систем, с учетом различных факторов их применения для защиты корпоративных систем. Представлена классификация критериев эффективности применения DLP-систем. Разработана математическая модель выбора эффективного DLP-решения, с учетом коэффициента защищенности и выявления утечки информации в ходе бизнес- процессов. Приведена структурная модель оценки эффективности DLP-систем, с учетом минимально допустимых параметров обнаружения утечек информации по различным каналам.

Ключевые слова: *DLP-система, бизнес-процесс, активная защита, оценка эффективности*

Shaburov A. S., Zhurilova E. E.

MODEL ASSESSING THE EFFECTIVENESS OF APPLICATION DLP-SOLUTIONS TO PROTECT CORPORATE SYSTEMS

In this article analyzes the options for assessing the effectiveness of DLP-systems, taking into account of the various factors of their application to protect corporate systems. It show the classification of criteria efficiency of application of DLP-systems. It working out a mathematical model of choice DLP-effective solutions, taking into account the factor of security and detection of information leakage in the course of business - processes.Show the block model evaluation of the effectiveness of DLP-systems, taking into account the minimum permissible parameters of information leakage detection through various channels.

Keywords: *DLP-system,business process, active protection, performance evaluation*

В условиях растущего количества угроз информационной безопасности борьба с утечками информации в корпоративных системах предприятий и организаций остается одной из актуальных задач[1]. Прежде всего, это связано с необходимостью поддержания устойчивости реализации бизнес-процессов, обеспечивающих экономическую и финансовую стабильность хозяйствующих субъектов. В настоящее время рынок средств защиты информации от утечек представляет собой выбор разнообразных решений[2]. Однако, по-

добрать эффективное средство борьбы с утечками информации, подходящее для конкретного предприятия, зачастую является трудной задачей. Это заставляет собственников информационных ресурсов руководствоваться предложениями конкретных разработчиков DLP-систем, зачастую преследующими коммерческую выгоду и не всегда учитывающими особенности функционирования корпоративных систем[3].

Выбор средства противодействия утечкам информации среди DLP-системможет быть основан на различных подходах. Основным фактором для выбора DLP-решения является фактор количественного выявления каналов утечки информации. Кроме того, выбор может осуществляться как с учетом нормативно-правовых аспектов внедрения DLP-системы[4], так и с учетом особенностей применяемого для выявления угрозы алгоритмов морфологического анализа[5] и ряда других параметров. В то же время опыт внедрения, эксплуатации и оценки подобных систем позволили сформировать основные, базовые группы критериев оценки эффективности.

Так, по информации от независимой исследовательской компании Forrester Research, выделяются четыре критерия оценки эффективности DLP-систем[6]:

- многоканальность;
- унифицированный менеджмент;
- активная защита;
- классификация информации с учетом, как ее содержимого, так и контекста самой информации.

Сущность предлагаемых критериев заключается в следующем. Критерий многоканальности представляет собой требование к DLP-системе охватывать максимально возможное количество каналов утечки информации, начиная от e-mail и заканчивая файловыми операциями.

Следующим критерием является унифицированный менеджмент, представляющий собой наличие единого средства управления всеми компонентами, входящими в состав DLP-системы. В качестве примера реализации этого требования можно назвать возможность управления тремя основными компонентами системы с одной консоли: сервером баз данных, устройством перехвата и агентами на рабочих станциях.

Критерий активной защиты подразумевает наличие возможности реагировать на утечку информации не только пассивно, фиксируя ее факт, но и активно, блокируя канал утечки информации.

Суть четвертого критерия основывается на фиксации не только содержимого документов с конфиденциальной информацией, но и их атрибутов, например, используемого протокола, отправителя, получателя и т.д.

Данный перечень критериев эффективности DLP-системы не является исчерпывающим. Рассмотрим другой их набор, также используемый дляоценки защиты от утечек информации[7]:

- количество ложных срабатываний (ошибки первого рода);

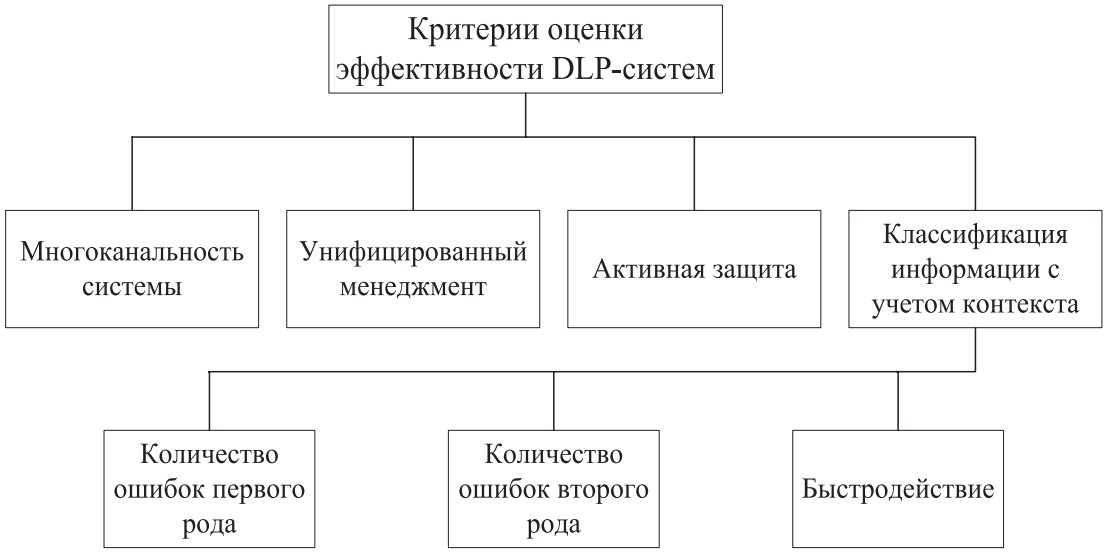

Рис. 1. Критерии оценки эффективности DLP-систем

- количество пропущенных утечек информации (ошибки второго рода);
- быстродействие DLP-системы.

Критерии количества ложных срабатываний и количества пропущенных утечек информации напрямую связаны с качеством морфологического анализа текстов DLP-системамис учетом, как содержимого, так и контекста самой информации.

Быстродействие DLP-системы зависит от объемов обрабатываемой информации и корректности составленных правил обработки информации, чем корректнее составлены правила, тем меньше ошибок и ложных срабатываний и тем меньше количество времени, требуемое для выяснения истины.

Представим классификацию критериев оценки эффективности применения DLP-системы в корпоративных сетях, объединив рассмотренные выше классификации, с учетом детализации контекстного анализа (рис. 1).

Сравним четыре наиболее популярных DLP-решения от разных производителей на соответствие приведенным выше критериям эффективности. Поскольку основной функционал DLP-решений сходен, необходимо будет уточнить и расширить приведенные критерии оценки эффективности. В таблице 1 будут рассмотрены только те критерии, оценка которых не требует практического применения моделей.

Возможность мониторинга нескольких каналов передачи данных, как правило, присутствует во всех современных DLP-системах, поэтому в таблице будет оценена так же возможность контроля таких специфических каналов утечки как BitTorrent, QIP, Skype и т.д.

Так же необходимо расширить показатели критерия «Активная защита», обозначив варианты реагирования на инциденты информационной безопасности.

Таблица 1

Сравнение DLP-решений

	Гарда Предприятие	Search Inform	Device Lock DLP	Falcongaze Secure Tower
Многоканальность				
IMAP4S	-	+	-	-
Протоколы авторизации и аутентификации	+	-	-	+
MMP(Mail.ru Агент)	+	+	+	+
XMPP(QIP, Jabber)	+	+	+	+
Skype	+	+	+	+
MS Lync	+	+	+	+
MySpace IM	-	+	-	+
BitTorrent	-	-	-	+
Web траффик в облаке	-	-	-	+
Унифицированный менеджмент				
	+	+	+	+
Активная защита				
Блокировка отправки данных на локальные устройства	+	+	+	+
Запрет доступа к данным для заданных приложений	+	+	-	-
Перемещение конфиденциальных данных в карантин	-	-	+	-
Ограничение доступа в зависимости от типа съемного носителя	+	+	+	+
Блокирование нежелательных процессов	+	+	-	+

Таблица 2

Результаты оценки соответствия критериям эффективности

	Гарда Предприятие	SearchInform	DeviceLockDLP	Falcongaze SecureTower
S%	67%	73%	53%	80%

Проведем оценку соответствия рассматриваемых систем представленным критериям и представим результат в процентном соотношении, результат 100% будет означать максимальное соответствие. Для оценки соответствия воспользуемся следующим соотношением:

$$S_{\%} = \frac{N_{+}}{N} \cdot 100\%,$$

где $S_{\%}$- процент соответствия;

N_{+} - количество положительных результатов по сравнению с критериями;

N – общее количество критериев.

Результаты полученных расчетов представлены в таблице 2.

На основании проведенной оценки выявлено, что наибольшим соответствием по выбранным критериям обладает DLP-система FalcongazeSecureTower, наименее – система DeviceLock.

С другой стороны, DLP-система, обладающая множеством определенных свойствдля реализации основной функции (обеспечить защиту от утечки информации), может отличаться по ряду дополнительных характеристик. К данным характеристикам могут относиться, как рассмотренные ранее в числе критериев эффективности, так и обусловленные свойствами среды применения системы. Условия среды применения системы, в свою очередь, могут способствовать проявлению конкретных угроз безопасности информации, а такжеобусловлены особенностями, протекающих в информационной системе, как отдельных бизнес-операций, так и бизнес-процессов, в целом. Математически это может быть сформулировано в следующем виде:

$$D = \sum_{i=N} K_i m_i, \sum_{i=N} K_i = 1, \qquad (1)$$

где:

D - обобщенный показатель оценки качества DLP - решения (обобщенный коэффициент защищенности, показывающий уровень выявления утечек информации по всей совокупности возможных каналов);

m_i-i-й частный показатель оценки эффективности DLP (частный коэффициент защищенности, показывающий, какой каналутечки i-го вида выявляется);

N-множество частных показателей оценки качества, сводимых в обобщенный показатель;

K_i- весовой коэффициент i-го частного показателя качества в аддитивной свертке.

Коэффициент защищенности (выявления утечки информации) в ходе отдельных бизнес-операций W_b может быть представлен выражением:

$$W_b = 1 - \frac{\sum_{j \in B} P_j \sum_{i \in N_j} \lambda_{ij} t_j (1 - m_i)}{\sum_{j \in B} P_j \sum_{i \in N_j} \lambda_{ij} t_j} \qquad (2)$$

где N_j- количество наиболее вероятных информационных угроз для j-го бизнес-процесса, связанного с утечкой информации;

m_i - коэффициент защищенности, показывающий, какой каналутечки i-го вида выявляется за счет применения DLP-системы;

λ_{ij}- интенсивность возможных утечек информациив ходе j-гобизнес-процесса $(i \in N_j)$, для $i \notin N_j$, $\lambda_{ij} = 0$;

t_j - время выполнения j-ой бизнес–операции;

B - количество бизнес - операций в бизнес-процессе;

P_j - вероятность выполнения бизнес-операцийjв бизнес-процессе B.

Для проведения экспериментальной оценки эффективности DLP-решения необходимо смоделировать ситуации передачи конфиденциальной информации, в различных форматах, по различным каналам связи.

На рис. 2 представлена искомая структурная модель оценки эффективности DLP- решения. Каналы перехвата информации, в общем случае, можно разделить на внутренние и внешние. К внутренним каналам относятся каналы, сформированные при передаче информации между персональными компьютерами в локальной сети предприятия и внешними носителями, функционирующими в

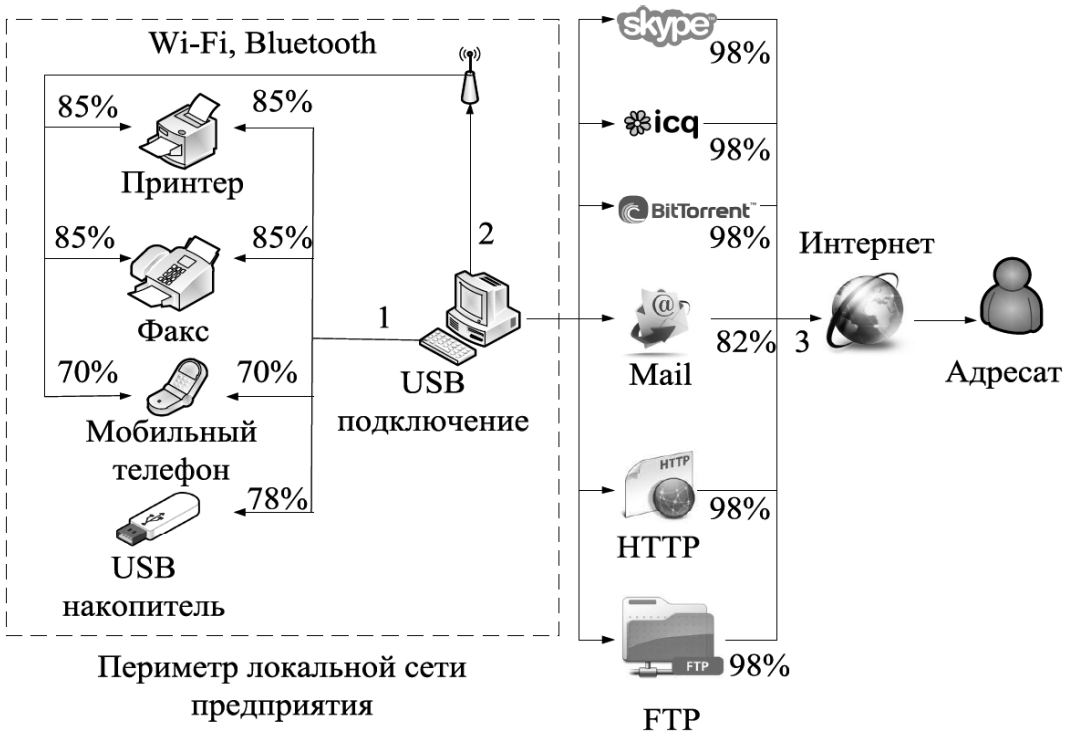

Рис. 2. Структурная модель оценки эффективности DLP-систем

пределах локальной сети (USB-накопители, сетевые принтеры и факсы). Взаимодействия по проводным и беспроводным каналам локальной сети показаны на рис. 2 стрелками 1 и 2, соответственно.

К внешним каналам целесообразно отнести почтовые сервисы, наиболее популярные мессенджеры, такие как Skype, ICQ, облачные сервисы и torrent. Передачу данных через сеть международного информационного обмена обозначены стрелкой 3.

Для проведения количественной оценки эффективности DLP-системы с использованием разработанной модели, необходимо задать допустимые параметры обнаружения утечек информации по каналу. Допустимые параметры обнаружения утечек информации по каналу определяются, как процентное соотношение выявленных утечек ко всем утечкам по каналу, при котором защита канала будет считаться эффективной. Минимальные допустимые параметры обнаружения утечек информации по различным каналам выберем на основании статистики по каналам утечек за первое полугодие 2016 года[8], основываясь на следующем принципе: чем больше процент утечек по данному каналу, тем выше должен быть минимальный допустимый параметр обнаружения утечек.

Экспериментальная оценка эффективности реагирования DLP-системы на инциденты предполагает реализацию следующей последовательности действий:

1. Настройка политики реагирования на инциденты в соответствии с руководством администратора к конкретной DLP-системе.

2. Имитирование нарушения политики безопасности (инцидента безопасности), посредством отправки конфиденциальной информации по случайно выбранному каналу связи.

3. Оценка адекватности реагирования DLP-системы, с регистрацией следующих событий:

- обнаружение инцидента безопасности;
- определение источника утечки информации;
- действия по блокированию канала утечки.

Этот перечень действий необходимо провести для каждого регулируемого канала информационного взаимодействия и провести суммарную оценку эффективности реагирования DLP-системы. Для проведения количественной оценки, с учетом имитирования протекающих в информационной системе бизнес-процессов предполагается использо-

вание выражений (1,2). На основании данной модели целесообразно дальнейшее проведение практических исследований эффективности работы DLP-систем.

Таким образом, анализ критериев оценки эффективности DLP-систем позволил осуществить сравнение нескольких наиболее известных решений на соответствие заданным критериям. Разработанная модель оценки эффективности применения DLP-систем позволяет оптимизировать процесс выбора наилучшего решения для корпоративной сети на основании задаваемых критериев оценки, что, в конечном итоге способствует повышению уровня защищенности информационных систем на практике.

Примечания

1. Утечка информации – современная угроза бизнесу// Журнал «InformationSecurity/ Информационная безопасность», №5 2011. URL: http://www.itsec.ru/articles2/Oborandteh/ytechka-informacii-sovremennaya-ygroza-biznesy (дата обращения: 1.11.2016).

2. Обзор решений для защиты от утечек информации// Журнал «InformationSecurity/ Информационная безопасность», №3 2016. URL: http://www.itsec.ru/imag/insec-3-2016/ (дата обращения: 1.11.2016).

3. Шабуров А.С., Журилова Е.Е., Лужнов В.С. Технические аспекты внедрения DLP – системы на основе FalcongazeSecureTower // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – Пермь, 2015. - № 16. – С. 57 - 67.

4. Шабуров А.С., Журилова Е.Е. О нормативно-правовых аспектах внедрения DLP – систем // Вестник УрФО. Безопасность в информационной сфере. – Челябинск, 2015. – № 3(17). – С.37 – 41.

5. Шабуров А.С., Журилова Е.Е. Особенности реализации алгоритмов морфологического анализа в DLP-системах // Вестник УрФО. Безопасность в информационной сфере. – Челябинск, 2016. – № 2(20). – С.23 – 28.

6. Персональный сайт компании TopSBusinessIntegrator [Электронный ресурс]. 2001 – 2012. URL: http://www.topsbi.ru/default.asp?trID=1206 (дата обращения: 3.11.2016).

7. Кумунжиев К.В., Зверев И.Н. Метод повышения эффективности dlp-системы при семантическом анализе и категоризации информации // Современные проблемы науки и образования. – 2014. – № 5. URL: http://www.science-education.ru/ru/article/view?id=14741 (дата обращения: 13.11.2016).

8. Исследование утечек информации в первом полугодии 2016 года [Электронный ресурс]. – URL: https://www.infowatch.ru/report2016_half (дата обращения: 16.11.2016).

ШАБУРОВ Андрей Сергеевич, кандидат технических наук, доцент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета, 614990, Пермь, Комсомольский пр., 29. E-mail: shans@at.pstu.ru.

ЖУРИЛОВА Елена Евгеньевна, студент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета, 614990, Пермь, Комсомольский пр., 29. E-mail: ele11485995@yandex.ru.

SHABUROV AndreySergeevich, PhD of Technical Sciences at the Department of Automation and Telemechanics, Perm National Research Polytechnic University, 614990, 29, Komsomolsky prospect, Perm. E-mail: shans@at.pstu.ru.

ZHURILOVA Elena Evgen'evna, student at the Department of Automation and Telemechanics, Perm National Research Polytechnic University, 614990, 29, Komsomolsky prospect, Perm. E-mail: ele11485995@yandex.ru.

УДК 003.26 + 004.057.4 Вестник УрФО № 4(22) / 2016, с. 21–25

Бортник Д. А., Кротова Е. Л., Савочкина А. А.

КЛАССИФИКАЦИЯ РЕАЛИЗАЦИЙ ПРОТОКОЛОВ ТАЙНОГО ГОЛОСОВАНИЯ

В статье приведены основные требования, предъявляемые к протоколам тайного голосования. Рассмотрены несколько разновидностей абстрактных протоколов – простейший протокол голосования с центром подсчета голосов, усложненный протокол голосования с центром подсчета голосов, протокол голосования со слепыми подписями. Указаны основные недостатки данных схем голосования. Далее рассмотрены два реальных протокола голосования – Fujioka-Okamoto-Ohta и He-Su. Также описаны их преимущества и недостатки.

Ключевые слова: *протокол тайного голосования, слепая подпись, протокол He-Su, протокол Fujioka-Okamoto-Ohta.*

Bortnik D. A., Krotova E. L., Savochkina A. A.

CLASSIFICATION OF THE SECRET VOTING PROTOCOLS

The main requirements imposed to protocols of ballot are adduced in the article. The several versions of abstract protocols are considered. For example, the elementary protocols of ballot with counting center, complicated protocol of ballot with counting center and protocols with blind signatures. The main disadvantages of these schemes of ballot are specified. Then two present protocols of ballot are considered – Fujioka-Okamoto-Ohta and He-Su. Their advantages and disadvantages are also described.

Keywords: *protocol of ballot, blind signature, protocol He-Su, protocol Fujioka-Okamoto-Ohta.*

Введение

В некоторых странах, например, Эстонии, Бельгии, Франции, Норвегии и других[1], возможность электронного голосования предусмотрена законодательством. Однако следует отметить, что электронное голосование никогда не будет внедрено, если не будет разработан надежный протокол, удовлетворяющий ключевым требованиям[2]. Таким образом, протоколы тайного голосования являются одним из типов современных прикладных криптографических протоколов.

Можно выделить несколько основных требований, предъявляемых к данным протоколам:

1. Голосовать могут только легальные избиратели;

2. Каждый избиратель может проголосовать только один раз;

3. Избиратели не могут проголосовать вместо кого-то другого;

4. Голосование является тайным;

5. Никто не может изменить чужой голос;

6. Каждый голосующий может проверить, что его голос был учтен при подведении итогов.

Протоколы тайного голосования можно разделить на 2 группы: децентрализованные и централизованные.

В децентрализованных протоколах взаимодействуют только избиратели без участия какого-либо центрального органа. Недостатком протоколов этой группы является их сложность с точки зрения количества вычислений и количества пересылаемой информации, из-за чего уже при сравнительно небольшом k они практически невыполнимы[2]. В централизованных протоколах создается центр подсчета голосов. Особенностью протоколов данной группы является тот факт, что центр должен быть честным и пользоваться безусловным доверием избирателей[3].

Рассмотрим протоколы обеих групп и выявим их характерные черты.

Простейший протокол голосования с центром подсчета голосов

Данный протокол основывается на схеме ассиметричного шифрования. Электронные выборы с помощью него можно разделить на 3 этапа[2]:

1) Избиратель шифрует свой бюллетень открытым ключом Центральной избирательной комиссии (ЦИК)

2) Избиратель посылает зашифрованный бюллетень ЦИК

3) ЦИК расшифровывает бюллетень закрытым ключом, подводит итоги и опубликовывает результаты

На рисунке 1 изображен принцип работы протокола. Public key и private key – открытый и закрытый ключи ЦИК соответственно.

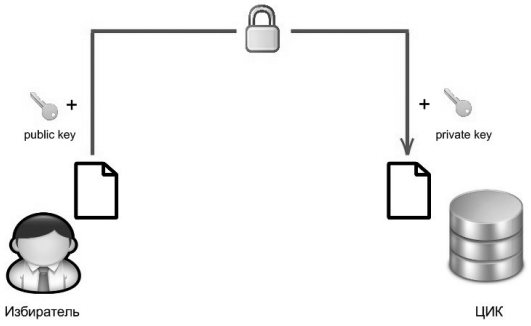

Рис. 1. Простейший протокол электронного голосования

У этой схемы отсутствует процедура аутентификации избирателей, из-за чего становится невозможным отследить легальность голосующих и их уникальность (любой избиратель может проголосовать сколько угодно раз). Положительной стороной протокола является невозможность изменить голос другого избирателя, но, ввиду описанных выше недостатков, это является не таким важным.

Усложненный протокол голосования с центром подсчета голосов

Кроме ассиметричного шифрования в усложненном протоколе используется электронная подпись избирателя. Процесс голосования можно разбить на 4 этапа[2]:

1) Избиратель подписывает бюллетень своим закрытым ключом;

2) Избиратель шифрует свой бюллетень открытым ключом Центральной избирательной комиссии (ЦИК);

3) Избиратель посылает зашифрованный бюллетень ЦИК;

4) ЦИК расшифровывает бюллетень, проверяет подпись, подводит итоги и опубликовывает результаты.

На рисунке 2 изображен принцип работы усложненного протокола. Public key 1 и private key 1 –ключи избирателя, public key 2 и private key 2 –ключи ЦИК.

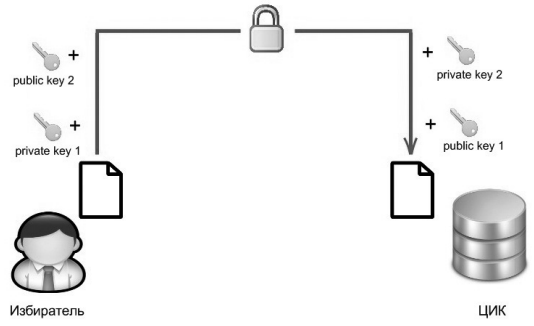

Рис. 2. Усложненный протокол электронного голосования

Данная схема позволяет аутентифицировать избирателя и удостовериться в том, что каждый голосовал не более одного раза. В этом алгоритме присутствуют недостаток – ЦИК знает, за кого проголосовал каждый избиратель. Чтобы данный протокол работал, необходимо, чтобы избиратели полностью доверяли ЦИК.

Протокол голосования со слепыми подписями

Аутентификацию избирателей, не нарушающую принципа тайного голосования, можно реализовать с использованием слепой подписи[4, 5].

В выборах участвуют три стороны: избиратель, валидатор и счетчик (например, ЦИК). Валидатор – сторона, проверяющая уникальность избирателя и подписывающая его бюллетень. Счетчик – сторона, подсчитывающая результаты голосования. Валидатор не должен знать кандидата, за которого проголосовал избиратель, а счетчик не должен знать личность избирателя.

Процесс голосования можно разделить на 7 этапов.

1) Избиратель и валидатор устанавливают надежное соединение со взаимной аутентификацией;

2) Избиратель создает бюллетень, голосует за произвольного кандидата, добавляет к бюллетеню уникальную последовательность и хеширует бюллетень;

3) Избиратель добавляет к хешу маскирующий множитель и отправляет на подпись к валидатору;

4) Валидатор проверяет уникальность избирателя (избиратель не должен голосовать более одного раза) и подписывает полученное сообщение;

5) Избиратель извлекает маскирующий множитель и получает корректную подпись для хеша бюллетеня;

6) Избиратель анонимно отправляет подписанный хеш счетчику;

7) Счетчик проверяет подпись и подводит итоги.

Слепую подпись можно реализовать разными способами, например, с помощью алгоритма RSA[2] или с использованием криптографии на эллиптических кривых[6].

У описанной выше схемы также присутствуют недостатки. Если на этапе (6) избиратель отошлет бюллетень не анонимно, ЦИК сможет узнать, кто за кого голосовал. Кроме того, ЦИК может создать любое число правильных и подписанных бюллетеней и смошенничать, прислав их сама себе. И если какой-либо избиратель обнаружит, что бюллетень был подменен, он не сможет этого доказать[2].

Рассмотрим также несколько реальных протоколов тайного голосования.

Протокол Fujioka-Okamoto-Ohta

Протокол Fujioka-Okamoto-Ohta[7] основывается на рассмотренном выше протоколе голосования со слепыми подписями. В голосовании так же участвуют избиратель, валидатор (администратор) и счетчик.

Процесс голосования можно разбить на 7 этапов:

1) - Администратор утверждает списки легитимных избирателей.

2) - Избиратель генерирует пару ключей e_{public} и $e_{private}$ и секретный ключ e_{secret};

- Ставит свой голос в бюллетене B;

- Шифрует бюллетень ключом e_{secret} – encrypt(e_{secret}, B);

- Маскирует зашифрованный бюллетень – blind(encrypt(e_{secret}, B));

- Шифрует результат личным ключом - blind(sign($e_{private}$, encrypt(e_{secret}, B)));

- Отправляет полученное сообщение администратору.

3) - Администратор создает пару ключей v_{public} и $v_{private}$;

- Удостоверяется в действительности бюллетеня;

- Подписывает полученное сообщение M личным ключом – sign($v_{private}$, M);

- Возвращает результат избирателю.

4) - Избиратель снимает с подписанного бюллетеня маскировку в силу коммутативности слепой подписи - sign($v_{private}$, sign($e_{private}$, encrypt(e_{secret}, B)));

- Отправляет получившееся сообщение счетчику (анонимно);

5) - Счетчик проверяет подписи избирателя и администратора;

- Помещает зашифрованный бюллетень encrypt(e_{secret}, B) в список, который будет опубликован после того, как закончится заранее оговоренный срок.

6) - Избиратель анонимно посылает счетчику ключ e_{secret} и номер строки, в которой находится его бюллетень.

7) - Счетчик расшифровывает бюллетень;

- Подсчет результатов.

Как указано в примечании авторов[7], возможна ситуация, когда избиратель посылает неверный ключ, который не может расшифровать бюллетень. В этом случае невозможно определить, кто является нечестным, избиратель или счетчик. Для предотвращения этого избирателям следует посылать ключи третьей, независимой стороне, например, кандидатам выборов, которые, скорее всего, не сотрудничают.

Протокол He-Su

Еще одним протоколом, основанным на идее слепой подписи, является протокол He-Su. Он удовлетворяет почти всем предъявляемым требованиям. В данном алгоритме участвуют три стороны – избиратель, администратор и счетчик. Но, в отличие от протокола Fujioka-Okamoto-Ohta, в схеме He-Su подписывается ключ избирателя, а не бюллетень.

Процесс голосования можно разделить на 10 этапов[8]:

1) - Избиратель генерирует пару ключей - D_v (закрытый) и E_v (открытый);

- Генерирует случайное число R (маскирующий множитель);

- Вычисляет $E_a(R) * (h(E_v))$, где E_a – открытый ключ администратора, h – хеш-функция;

- Отправляет результат администратору.

2) - Проверяет приемлемость избирателя;

- Подписывает принятое сообщение: $D_a(E_a)R * D_a(h(E_v)) = R * D_a(h(E_v))$, где D_a – личный ключ администратора.

- Отправляет результат избирателю;

- Публикует список авторизованных избирателей.

3) - Избиратель убирает маскирующий множитель R из полученного сообщения;

- Проверяет равенство $E_a(D_a(h(E_v))) = h(E_v)$;

- При верном равенстве избиратель убеждается в том, что имеет подписанный ключ.

4) - Избиратель отправляет счетчику E_v и $D_a(h(E_v))$.

5) - Счетчик проверяет равенство $E_a(D_a(h(E_v))) = h(E_v)$;

- При верном равенстве счетчик авторизует ключ E_v;

- Публикует список авторизованных ключей.

6) - Избиратель отправляет счетчику E_v, $K_v(B_v)$, $D_v(h(K_v(B_v)))$, где K_v – секретный ключ избирателя (для симметричного шифрования), B_v – бюллетень;

7) - Счетчик проверяет, является ли ключ E_v авторизованным;

- Проверяет равенство $E_v(D_v(h(K_v(B_v)))) = h(K_v(B_v))$;

- При положительном результате публикует E_v, $K_v(B_v)$, $D_v(h(K_v(B_v)))$.

8) - Избиратель проверяет в опубликованном счетчиком листе наличие записи о своем голосе (из пункта 7);

- В случае отсутствия записи обращается в соответствующие органы.

9) - Избиратель отправляет счетчику E_v, K_v, $D_v(h(K_v))$;

10) - Счетчик проверяет равенство $E_v(D_v(h(B_v))) = h(B_v)$;

- В случае равенства получает бюллетень $K_v^{-1}(K_v(B_v)) = B_v$;

- Публикует информацию: B_v, $K_v(B_v)$, K_v, $D_v(h(K_v(B_v)))$, $D_v(h(K_v))$, E_v.

К преимуществам протокола He-Su можно отнести возможность избирателя изменить свой голос во время выборов. Избиратель может сделать это, не раскрывая свой бюллетень. Кроме того, протокол достаточно прост и имеет малую вычислительную сложность[8].

Заключение

Протоколы тайного голосования основываются на широко известных и проверенных алгоритмах шифрования, хеширования, цифровой подписи. Но для претворения их в жизнь необходимо учесть множество требований и факторов. Реализация какого-либо требования, предъявляемого к данным протоколам, может стать хорошей задачей для дальнейшего исследования .

Примечания

1. Антонов Я. В. Международный опыт электронного голосования // Сборник конкурсных работ в области избирательного права и избирательного процесса выполненных студентами, аспирантами в 2010/2011 учебном году. М.: РЦОИТ. 2011.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Триумф, 2002. — 816 с.

3. Введение в криптографию / Под общ. ред. В. В. Ященко. - 4-е изд., доп. М.: МЦНМО, 2012. - 348 с.

4. Клюжев А. Электронное голосование [Электронный ресурс] // Gosbook.ru. – URL: http://www.gosbook.ru/node/28337 (дата обращения: 13.06.2016).

5. Иванов Е. Слепая подпись на основе ГОСТ 34.10-2001 [Электронный ресурс] // Habrahabr.ru. – URL: https://habrahabr.ru/post/136022/ (дата обращения: 13.06.2016).

6. Козина Г. Л., Никулищев Г. И. Протокол слепой подписи на основе ГОСТ Р 34.10-2012 [Электронный ресурс] // Aticmd.md. – URL: http://www.aticmd.md/wp-content/uploads/2014/04/V_2_33_MMOTI_Kozina.pdf (дата обращения: 13.06.2016).

7. Fudjioka A., Okamoto T., Ohta K. A Practical Secret Voting Scheme for Large Scale Elections [Электронный ресурс] // Csail.mit.edu. – URL: https://people.csail.mit.edu/rivest/voting/papers/FujiokaOkamotoOhta-APracticalSecretVotingSchemeForLargeScaleElections.pdf (дата обращения: 17.06.2016).

8. He Q., Su Z. A New Practical Secure e-Voting Scheme [Электронный ресурс] // Cs.cmu.edu. – URL: http://www.cs.cmu.edu/~qihe/paper/e_voting (дата обращения: 17.06.2016).

БОРТНИК Дмитрий Аркадьевич, студент Пермского национального исследовательского политехнического университета. 614990, г. Пермь, Комсомольский пр-кт, 29. E-mail: bortnikdmitriy@mail.ru.

КРОТОВА Елена Львовна, кандидат физико-математических наук, доцент кафедры высшей математики Пермского национального исследовательского политехнического университета. 614990, г. Пермь, Комсомольский пр-кт, 29. E-mail: lenkakrotova@yandex.ru.

САВОЧКИНА Анна Александровна, старший преподаватель кафедры высшей математики Пермского национального исследовательского политехнического университета. 614990, г. Пермь, Комсомольский пр-кт, 29. E-mail: aidas_76@mail.ru.

BORTNIK Dmitrii Arkad'evich, is a student of Perm National Research Polytechnic University. 614990, Perm, 29, Komsomolsky pr. E-mail: bortnikdmitriy@mail.ru.

KROTOVA Elena L'vovna, is a Ph. D. in Physico-Mathematical Sciences, Associate Professor, Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm, 29, Komsomolsky pr. E-mail: lenkakrotova@yandex.ru.

SAVOCHKINA Anna Alexandrovna, is a senior lecturer, Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm, 29, Komsomolsky pr. E-mail: aidas_76@mail.ru.

УДК 004.032.26 + 342.7 : 004.056.5 Вестник УрФО № 4(22) / 2016, с. 26–30

Трунин А. М., Рагозин А. Н.

НЕЙРОННЫЕ СЕТИ В ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Защита персональных данных является актуальной проблемой в сфере информационной безопасности. Персональные данные, такие как идентификационные коды кредитных карт, данные паспорта, номера банковских счетов, хранящиеся в электронном виде с использованием электронных каталогов или баз данных, требуют уникального подхода к защите информации и быстрой реакции на их изменение или использование. Данная работа рассматривает применение нейронных сетей: самоорганизующихся сетей Кохонена, иерархического кластер-анализа и нейронных сетей специальной архитектуры в защите и обработке большого числа персональных данных, содержащихся в каталогах или базах данных.

Ключевые слова: *защита информации, информация, персональные данные, кластер-анализ, нейронные сети.*

Trunin A. M., Ragozin A. N.

NEURAL NETWORKS IN THE PROTECTION OF PERSONAL DATA

Protection of personal data is an actual problem in the field of information security. Personal data, such as the identity of the credit card codes, passport details, bank account numbers stored in electronic form with the use of electronic catalogs or databases require a unique approach to data protection, and rapid response to changing them or use. This work considering the use of neural networks: self-organizing Kohonen networks, hierarchical cluster analysis and neural network with special architecture in protection and processing of a large number of personal data contained in directories or databases.

Keywords: *Data protection, information, personal data, cluster analysis, specific neural network.*

Нейронные сети способны обрабатывать огромные массивы данных по определенным, необходимым для решения задачи, правилам. От правильно подобранного типа нейросети зависит качество решения задачи. Далее рассмотрены основные типы нейронных сетей и иерархического кластер анализа, применяющиеся в решении задач защиты данных.

Нейронные сети Кохонена– класс нейронных сетей, основным элементом которых является слой Кохонена[3]. Слой Кохонена состоит из адаптивных линейных сумматоров («линейных формальных нейронов»). Как правило, выходные сигналы слоя Кохонена обрабатываются по правилу «победитель получает всё» - наибольший сигнал превращается в единичный, остальные обращаются в ноль[3].

Слой Кохонена состоит из некоторого количества параллельно действующих линейных элементов. Все они имеют одинаковое

число входов и получают на свои входы один и тот же вектор входных сигналов. На выходе j-го линейного элемента получаем сигнал:

$$y_j = \omega_{j0} + \sum_{i=1}^{m} \omega_{ji} x_i \qquad (1)$$

где:

- ω_{ji} – весовой коэффициент i–го входа j-го нейрона;
- i – номер входа;
- j – номер нейрона;
- ω_{j0} – пороговый коэффициент.

После прохождения слоя линейных элементов сигналы посылаются на обработку по правилу «победитель получает всё»: среди выходных сигналов выполняется поиск максимального нейрона[3]. Окончательно, на выходе сигнал с определенным номером равен единице, остальные – нулю. Если максимум одновременно достигается для нескольких сигналов, то:

- либо принимаются все соответствующие сигналы равными единице;
- либо равным единице принимают только первый сигнал в списке (по соглашению).

Кластер-анализ – это множество вычислительных процедур, которые формируют либо выявляют иерархии (разбиения), лежащие в основе тех или иных совокупностей данных. Анализ данных представляет собой множество вычислительных процедур, которые описывают, распознают или идентифицируют структуры, лежащие в основе скоплений точек, обычно принадлежащих пространству малой размерности, сконструированному по совокупности данных (многомерное шкалирование, факторный анализ и подобные методы).

Алгоритмы кластер-анализа в совокупности с самоорганизующимися сетями Кохонена представляют собой инструмент быстрой и качественной обработки информации, ее анализа и своевременной защиты[2].

Обработка персональных данных, их классификация и обеспечение их сопоставления между собой для дальнейшей защиты происходит в два этапа.

Первый этап – это анализ всех данных при помощи самоорганизующихся сетей Кохонена, классификация их и предоставление для дальнейшей обработки.

Вся представленная к обработке информация нормируется, то есть приводится к подобию на основе общих критериев для дальнейшего сопоставления данных между собой. Далее из нормированных данных формируется вектор входных данных, который подается на вход самоорганизующейся нейронной сети Кохонена.

Все данные, поданные в виде векторов, проходят процедуру «кластеризации», то есть делятся на группы «похожих» объектов, называемых кластерами. Кластеризация позволяет сгруппировать сходные данные, что облегчает их последующий анализ. Формально задача кластеризации описывается следующим образом: из множества объектов $I = \{i_1, i_2, \ldots, i_n\}$ каждый из которых характеризуется вектором $x_j = \{x_{j1}, x_{j2}, \ldots, x_{jm}\}$, j=1,2,…,n атрибутов (параметров).

Требуется построить множество кластеров C и отображение F множества I на множество C, то есть $F: I \to C$. Задача кластеризации состоит в построении множества

$$C = \{C_1, C_2, \ldots, C_k\}$$

где C_k – кластер, содержащий «похожие» объекты из множества I:

$$C_k = \{i_j, i_p | i_j \epsilon I, i_p \epsilon I \text{ и } d(i_j, i_p) < \sigma\}$$

σ – величина, определяющая меру близости для включения объектов в один кластер, $d(i_j, i_p)$ – мера близости между объектами, называемая расстоянием.

К требуемому объему информации, содержащему персональные данные, представляемые для обработки и своевременного анализа, применяется классификация[1] при помощи самоорганизующихся сетей Кохонена, которые обучаются самостоятельно на основе предоставленных данных. После прохождения данных через сеть Кохонена на выходе данные сортируются и выводятся в виде вектора $y(1)$.

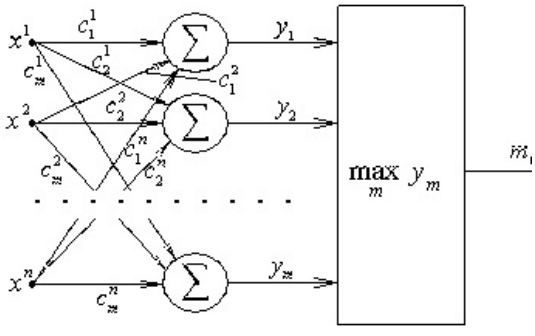

Рис. 1. Структура сети Кохонена

Второй этап – это интерпретация результатов, полученных при обработке данных нейронными сетями Кохонена, при помощи иерархического кластер-анализа.

Для этого вектор $y(1)$ проходит кодирование и описание данных (отбор и кодирование таблиц данных, первичную элементарную обработку, кодирование и выбор метрики), анализ и классификацию (структурирование и синтез, построение дендрограмм) и интерпретацию полученных результатов конкретным графическим представлением и дополнительным наглядным описанием. После проделанных процедур данные представляются в удобном и доступном для анализа виде с целью их критического исследования.

Для решения задач защиты данных, так же находят применение нейронные сети со специально-конструируемой структурой.

Общим для всех нейросетей является этап подготовки данных, а именно их нормировка, формирование входных векторов (данных для анализа) и создании целевой функции, на основе которой происходит обучение данной нейросети.

Главным отличием специальной нейронной сети от кластерного анализа и нейронных сетей Кохонена является возможность конструирования специальной структуры обработки данных для определенной задачи.

Для проведения анализа возможностей данных нейросетей и получения наглядных результатов был использован программный пакет «Matlab».

Первым этапом в формировании выбранной нейронной сети является нормирование входных и целевых данных для подачи на определенный тип нейросети.

Задание нейронной сети имеет определенный синтаксис:

net=network(numInputs,numLayers,biasConnect,inputConnect,layerConnect,outputConnect),

где:

- network – функция задания типа нейронной сети, в данном случае функция задания собственной нейросети пользователя;
- numInputs – определяет количество входов сети;
- numLayers – определяет количество слоев сети;
- biasConnect – определяет, какие слои имеют смещения;
- inputConnect - определяет, какие слои обладают связями со входами;
- layerConnect - определяет какие слои связаны с другими слоями;
- outputConnect - определяет какие слои генерируют выходы сети;

Для задания алгоритмов адаптации, инициализации, тренировки и оценки функционирования сети используются следующие функции:

- adaptFcn - определяет функцию, которая будет использована для адаптации сети (net.adaptFcn).
- initFcn - определяет функцию, используемую для инициализации матриц весов и векторов смещений сети (net.initFcn).
- performFcn – определяет функцию, используемую для оценки функционирования сети (net.performFcn).
- trainFcn - определяет функцию, используемую для тренировки сети (net. trainFcn).

Одной из самых важных задач в формировании нейронной сети является задача подбора правильной функции тренировки сети. Функции тренировки сети, доступные в программном пакете Matlab, позволяют задать требуемый для решения задачи процесс обучения и оптимизировать его выполнение. Ниже приведены некоторые функции обучения нейросети:

- trainb – пакетная тренировка с использованием правил обучения для весов и смещений;
- trainbfg – тренировка сети с использованием квази – Ньютоновского метода BFGS;
- trainc – использование приращений циклического порядка;

Листинг функции в программном пакете Matlab, задающей нейронную сеть с собственной архитектурой:

```
function net = create_network(inputs, outputs)
Создание сети
net = network();
net.numInputs = 1; Количество входов
net.numLayers = 2; Количество слоев, первый - скрытый, второй - выходной
Входы
net.inputs{1}.size = inputs;
net.inputs{1}.processFcns = {'removeconstantrows', 'mapminmax'};
```

```
    Выходы
    net.outputs{2}.processFcns = {'removeconstantrows', 'mapminmax'};
    Тренировка
    net.dividefcn = 'dividerand';
    net.divideParam.trainRatio = 70/100;     Часть выборой для тренировки
    net.divideParam.valRatio = 15/100;       Часть выборок для проверки
    net.divideParam.testRatio = 15/100;      Часть выборок для конечного
тестирования
    net.performFcn = 'mse';                  Функция оценки качества
    net.trainFcn = 'trainlm';                Функция тренировки
    net.trainParam.epochs = 500;             Максимальное количество итераций
    net.trainParam.goal = 0;                 Допустимая погрешность
    Функция адаптации
    net.adaptFcn = 'adaptwb';                Функция адаптации
    Инициализация
    net = init(net);
    end
```

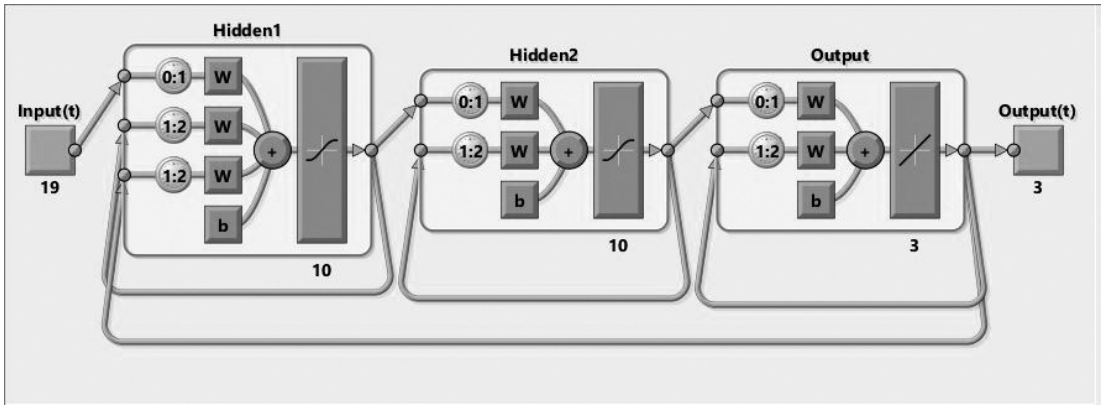

Рис. 2. Структура нейронной сети

Пример структуры нейронной сети приведен на рисунке 2.

Правильность выбора типа нейронной сети и функции обучения влияет на правильность решения и на качество защиты персональных данных пользователя. Благодаря своей гибкости, нейронные сети, сконструированные таким образом, позволяют решать задачи любой сложности и направленности, в том числе и задачи защиты данных.

Примечания

1. Мищенко Е. Ю., Соколов А. Н. Количественный анализ процедуры обезличивания персональных данных. Метод перемешивания // Вестник УрФО. Безопасность в информационной сфере /№ 3(21) / 2016, с. 30–37.

2. Жамбю М. Иерархический кластер-анализ и соответствия // Перевод с фр., 1988. С. 11–76.

3. Хайкин С. Нейронные сети: полный курс. – М.: Вильямс, 2006. – 1104 с.

ТРУНИН Андрей Михайлович, студент группы КЭ-437 высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский Государственный Университет» (Национальный исследовательский университет). Россия, 454080, г.Челябинск, проспект Ленина, д 76. E-mail: truninandrey@mail.ru.

РАГОЗИН Андрей Николаевич, научный рук., кандидат технических наук, доцент кафедры инфокоммуникационных технологий, доцент кафедры защиты информации ФГАОУ ВО «Южно-Уральский Государственный Университет» (Национальный исследовательский университет).Россия, 454080, г.Челябинск, проспект Ленина, д 76.

TRUNIN Andrey Mikhailovich, the student of higher School of Electronics and Computer Science of the FGAOU «South Ural State University» (National Research University). Russia, 454080, Chelyabinsk, Prospekt Lenina, 76. E-mail: truninandrey@mail.ru.

RAGOZIN Andrey, scientific chief., Ph.D., Candidate of Technical Sciences, assistant professor of information and communication technologies, assistant professor of information security FGAOU «South Ural State University» (National Research University). Russia, 454080, Chelyabinsk, Prospekt Lenina, 76.

УДК 342.951 Вестник УрФО № 4(22) / 2016, с. 31–34

Васильева А. А., Сутягин С. А., Полякова Е. Н., Москвин В. В.

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ГРАЖДАН ПРИ ПОДАЧЕ ЭЛЕКТРОННЫХ ОБРАЩЕНИЙ В ГОСУДАРСТВЕННЫЕ ОРГАНЫ

В статье рассмотрены проблемы обеспечения информационной безопасности персональных данных граждан РФ и пути их решения с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»[1].

В теории защита персональных данных (далее – ПДн) кажется довольно простой, но, как показывает практика, имеется множество проблем. Во-первых, передача данных, содержащих ПДн граждан, по незащищенным каналам, в связи с эти возникает возможность их перехвата злоумышленниками. Во-вторых, отсутствие криптографической защиты обращений. В-третьих, проблема аутентификации отправителя и т.д.

Ключевые слова: *Информационная безопасность, электронные обращения, федеральный закон, государственные органы.*

Vasilyeva A. A., Sutyagin S. A., Polyakova E. N., Moskvin V. V.

THE PROBLEMS OF INFORMATION SECURITY OF CITIZENS' PERSONAL DATA WHEN SUBMITTING ELECTRONIC APPLICATIONS TO THE STATE DEPARTMENTS

The problems of information security of personal data of citizens of Russia and ways to decide it into account the Federal law of 27.07.2006 № 152-FZ «On personal data».

The theory of personal data protection seems rather simple, but in practice, there are many problems. Firstly, data containing citizens' personal data over unprotected channels, there is a possibility of interception by hackers. Secondly, there is no cryptographic protection of applications. Third, there is the sender's authentication problem.

Keywords: *Information security, electronic treatment, the federal law, the state departments.*

Введение

В целях повышения качества и эффективности отношений органов власти и общественности Государственной Думой был принят Федеральный закон от 02.05.2006 N 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»[2]. Он регламентирует один из способов взаимодействия государства и общества. В связи с этим у граждан РФ есть возможность отправлять обращения в госорганы, представленные в виде предложений, заявлений или жалоб.

К сожалению, в законодательстве имеются недоработки, которые ставят под угрозу обеспечение информационной безопасности персональных данных (далее - ПДн) граждан.

Цель работы – исследование проблемы обеспечения информационной безопасности персональных данных граждан при подаче электронных обращений в государственные органы РФ, а также разработка эффективного механизма их защиты.

Нами был сформулирован ряд задач:

1. Исследовать проблемы, связанные с безопасностью персональных данных и их передачи.

2. Выявить основные угрозы для информационной безопасности ПДн.

3. Разработать и предложить к реализации комплекс соответствующих мер защиты.

Подача обращений через региональный сайт МФЦ

Для граждан РФ существует два способа подачи электронного обращения: с помощью заполнения формы на сайте органа местного самоуправления или на сайтах многофункциональных центров (далее - МФЦ), целью которых является автоматизация предоставления услуг населению.

В случае, когда пользователю необходимо отправить обращение через сайт МФЦ, их принуждают согласиться с передачей личных данных в открытом виде следующим условием: «Я подтверждаю свое согласие на передачу информации в электронной форме обращения (в том числе персональных данных) по открытым каналам связи сети Интернет».

При отказе пользователя действие не будет произведено. Причем на некоторых сайтах вообще может и не быть никакой информации об условиях передачи, либо она может быть затеряна в большом количестве другой информации.

Поэтому можно сделать вывод, что организация подобным образом снимает с себя ответственность за хищение личных данных граждан.

На рисунке 1 приведена реальная схема механизма подачи, перенаправления и ответа на электронные обращения. На первом этапе ПДн граждан РФ не защищены. Отношения же МФЦ и госорганов в информационной среде регулируются СМЭВ (т.е. «Единой системой межведомственного электронного взаимодействия»). Но при отправке ответа пользователю снова возникает угроза хищения личных данных.

Также на территории России действует Единый портал «Госуслуги», который тоже предоставляет различные функции и имеющий большую популярность среди населения. К сожалению, на нем не реализована услуга по подаче электронных обращений, что могло бы обеспечить информационную безопасность ПДн на первом этапе, в связи с тем что используется https-соединение.

Экспериментальная часть

В качестве доказательства наличия угрозы хищения ПДн, на базе кафедры «Безопасность информационных и автоматизированных систем» Курганского государственного университета было проведено два эксперимента. В качестве примера был выбран сайт московского филиала Многофункционального центра и рассматривалась атака MITM

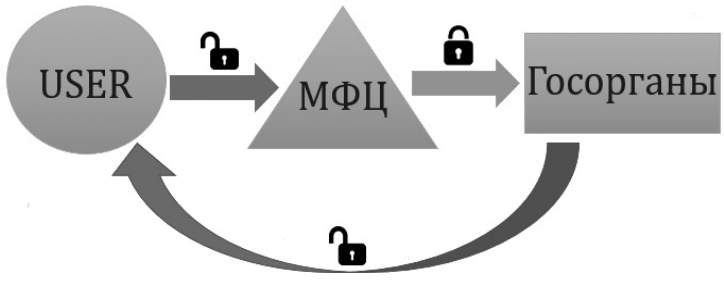

Рис. 1. Общая схема системы.

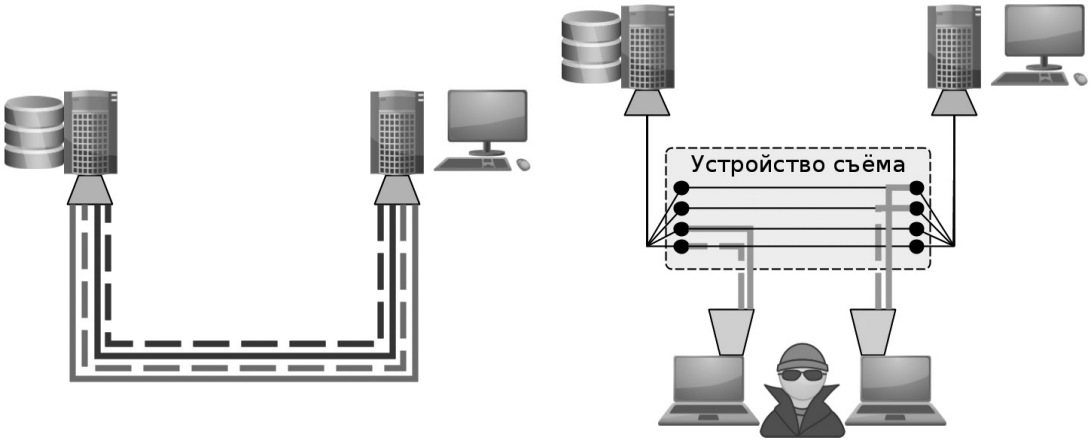

Рис. 2.
а) Общая схема работы кабеля 4-парного кабеля UTP категории 5е.
б) Принцип работы устройства съёма информации

(«Man in the middle») на узел пользователя, отправляющего свои данные через форму обращения на сайте.

В первом эксперименте использовалось специально подготовленное устройство (рис. 2), с помощью которого проводилась хакерская атака в условиях наличия прямого доступа к локальной сети атакуемого хоста. Во втором эксперименте съём информации производился непосредственно с кабеля с помощью двух контактных зажимов (рис. 3). В обоих случаях пакеты с информацией, введенной на форме, были перехвачены.

В ходе изучения данного вопроса обнаружили, что некоторые сайты, на которых предоставляется услуга формирования электронного обращения, например, сайты органов местного самоуправления, имеют аналогичную уязвимость.

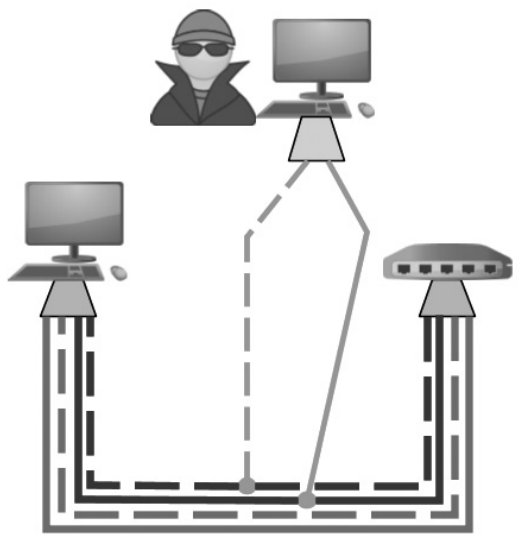

Рис. 3. Общая схема работы

Возникает проблема аутентификации личности отправителя и одним из способов решения данной проблемы это использование электронной цифровой подписи (далее ЭЦП). В связи с тем, что ЭЦП редко используется гражданами и имеется не у всех, ее стоимость довольно велика, то смысла ее приобретать для отправки всего одного обращения нет. Выходом из данной ситуации может быть наличие у МФЦ своей собственной электронной подписи, с помощью которой можно было бы бесплатно заверять документы граждан.

Для обеспечения равного доступа к рассматриваемой услуге, например, подача электронного обращения слабовидящими гражданами, должна существовать возможность формирования копии ответа для них шрифтом Брайля.

Заключение

Таким образом, в ходе исследования были выявлены проблемы, которые связаны не только с безопасностью передачи электронных обращений в госорганы, но и с другими аспектами.

Для обеспечения безопасности персональных данных, передаваемых по каналам сети Интернет, необходимо использовать:

- протоколы защиты VPN и TLS;
- программные и программно-аппаратные средства шифрования;
- средства электронной подписи.

Для проверки подлинности личных данных пользователя необходимо:

- отправлять обращения в виде электронного документа;
- использовать ЭЦП;
- заверять обращения с помощью собственной подписи МФЦ.

Для оптимизации эффективности МФЦ необходимо:

- создание общероссийской сети МФЦ;
- объединение всех центров на одном сайте с возможностью выбора региона;
- резервное копирование обращений и ответов на них для возможности получения ответа в другом регионе;
- организация региональных мобильных центров;
- добавить функцию формирования обращений на портале Госуслуги;
- рассылать SMS-уведомления о статусе обращений.

Примечания

1. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) «О персональных данных».

2. Федеральный закон от 02.05.2006 N 59-ФЗ (ред. от 03.11.2015) «О порядке рассмотрения обращений граждан Российской Федерации».

ВАСИЛЬЕВА Алена Алексеевна, студент кафедры «Безопасность информационных и автоматизированных систем» технологического факультета ФГБОУ ВО «Курганский государственный университет». 640020, г. Курган, ул. Советская, д. 63, стр.4. E-mail: alena.alekseyevna@yandex.ru

СУТЯГИН Сергей Александрович, студент кафедры «Безопасность информационных и автоматизированных систем» технологического факультета ФГБОУ ВО «Курганский государственный университет». 640020, г. Курган, ул. Советская, д. 63, стр.4. Email: svd.sergey95@gmail.com

ПОЛЯКОВА Елена Николаевна, кандидат педагогических наук, заведующий кафедры «Безопасность информационных и автоматизированных систем» технологического факультета ФГБОУ ВО «Курганский государственный университет». 640020, г. Курган, ул. Советская, д. 63, стр.4. E-mail: penelena1972@yandex.ru

МОСКВИН Владимир Викторович, старший преподаватель кафедры «Безопасность информационных и автоматизированных систем» технологического факультета ФГБОУ ВО «Курганский государственный университет». 640020, г. Курган, ул. Советская, д. 63, стр.4. E-mail: bias.kgsu.techno@gmail.com

VASILYEVA Alena Alekseyevna, student of the Department of «Security of information and automated systems» of the faculty of technology of the «Kurgan state University». 640020, Kurgan, Sovetskaya street, 63, p. 4. E-mail: alena.alekseyevna@yandex.ru

SUTYAGIN Sergey Alexandrovich, student of the Department of «Security of information and automated systems» of the faculty of technology of the «Kurgan state University». 640020, Kurgan, Sovetskaya street, 63, p. 4. Email: svd.sergey95@gmail.com

POLYAKOVA Elena Nikolayevna, the candidate of pedagogical Sciences, head of Department «Security of information and automated systems» of the faculty of technology of the «Kurgan state University». 640020, Kurgan, Sovetskaya street, 63, p. 4. E-mail: penelena1972@yandex.ru

MOSKVIN Vladimir Viktorovich, senior teacher of the Department «Security of information and automated systems» of the faculty of technology of the «Kurgan state University». 640020, Kurgan, Sovetskaya street, 63, p. 4. E-mail: bias.kgsu.techno@gmail.com

УДК 004.056.2 + 504.064.36(38) Вестник УрФО № 4(22) / 2016, с. 35–37

Ильин И. И., Зубов Я. М., Москвин В. В., Полякова Е. Н.

ИНТЕГРИРУЕМАЯ СИСТЕМА МОНИТОРИНГА

В статье представлен проект по реализации системы, решающей проблему необходимости мониторинга соответствующей инфраструктуры для обеспечения бесперебойности работы информационной системы. В результате анализа существующих на рынке решений был сделан вывод о необходимости расширения плана разработки системы созданием «модулей интеграции». Данные программные компоненты позволят быстро включать создаваемый продукт в существующие информационные инфраструктуры. Это станет значительным преимуществом по сравнению с аналогами. Традиционно такие решения представляют собой обособленную систему, имеющую собственный центр управления и набор протоколов, что создаёт необходимость изучения специальных интерфейсов управления и принципов взаимодействия.

Ключевые слова: *мониторинг, слежение, контроль среды, система мониторинга, контроль состояния среды, автоматизированная система управления, SCADA, архитектура клиент-сервер, веб-архитектура.*

Ilyin I. I., Zubov I. M., Moskvin V. V., Polyakova E. N.

INTEGRABLE MONITORING SYSTEM

This article presents a project about implementation of a system, which would solve the crucial need for appropriate infrastructure monitoring, for ensuring uninterrupted operation of information systems. As a result of a carried out analysis of solutions existing on the market, it was concluded that the system development plan needs to be expanded by creation of "integration modules". These software components are meant to enable fast integration into existing IT infrastructures. This will be a significant advantage in comparison with analogues. Traditionally, systems of this type are representing a separate system, having their own control center and protocols set, introducing a unique curve of learning the special interfaces and interaction priciples.

Keywords: *monitoring, tracking, environment control, monitoring system, environment monitoring, automated control system, SCADA, client-server, web architecture.*

Инновации в традиционных системах SCADA (англ. аббр. Supervisory Control and Data Acquisition – диспетчерское управление и сбор данных) зашли в тупик по трём основным причинам:

• программное обеспечение является слишком специфичным и узкоспециализированным;

• сложность внедрения SCADA-решений повышает порог вхождения;

• существующая модель лицензирования предполагает рост цены с ростом числа клиентов[1].

Наиболее существенный технологический недочёт – использование закрытых, понятных одному производителю протоколов. Доступная для всех альтернатива — открытый стандартизованный протокол HTTP (англ. аббр. Hypertext Transfer Protocol – протокол передачи гипертекста).

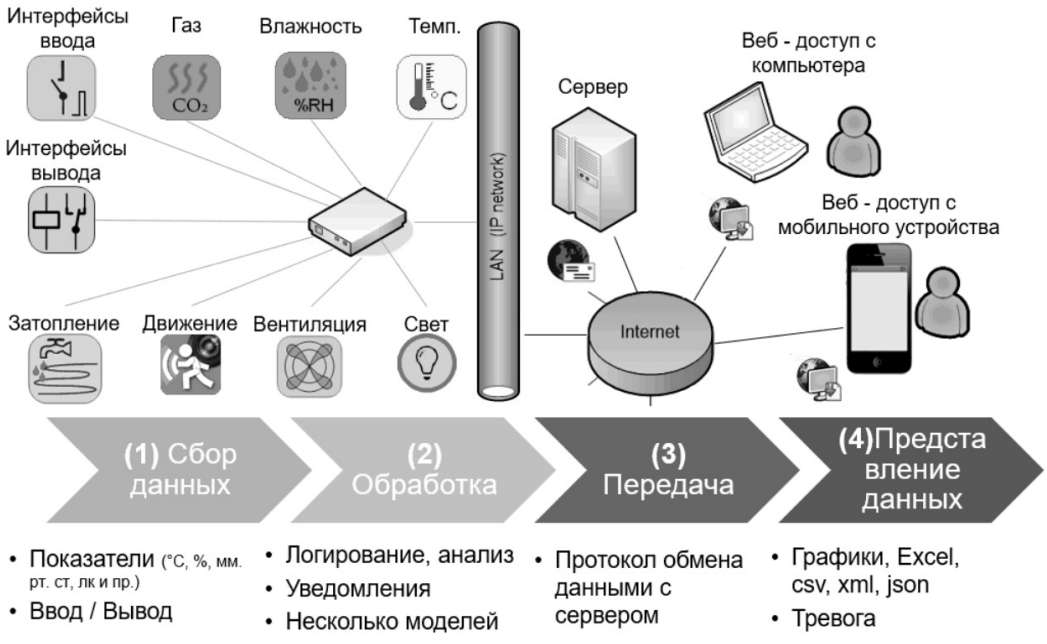

Рис.1. Функциональная модель системы

В ходе разработки решения предлагается использование архитектуры «клиент-сервер». Ключевая особенность данной архитектуры — то, что вычисления и обработка данных происходят на стороне сервера, что позволяет «сэкономить» на производственных мощностях клиентов. В качестве клиентского приложения используется, как правило, браузер. Посредством его клиент отправляет и принимает данные. На стороне сервера операции выполняются специальным программным обеспечением (веб-приложением), которое принимает запросы клиентов, обрабатывает их, формирует ответы. Показания датчиков передаются на сервер и в случае обращения отображаются на клиентском устройстве в виде графиков с текущими показаниями приборов (например, температуры, влажности, концентрации определённых типов газов в воздухе, освещённости, наличия затопления и движения). В процессе обработки запроса пользователя веб-приложение компонует ответ на основе исполнения программного кода, работающего на стороне сервера[2]. К операциям, выполняемым веб-приложением, относятся: приём и обработка данных от системы мониторинга и сохранение их на сервере; выполнение извлечения сведений из базы данных (далее — БД) по запросу пользователя; аутентификация пользователя и отображение интерфейса системы, соответствующего данному пользователю; отображение постоянно изменяющейся оперативной информации. Функциональная модель системы представлена на рисунке 1.

Веб-архитектура обладает заметными преимуществами, облегчающими процесс её реализации. Серверная часть системы с данной архитектурой не требовательна к производительности. Для переноса приложения на эту архитектуру требуется лишь приведение протокола взаимодействия сервера с клиентом к одному из веб-стандартов (к примеру, REST-API (англ. аббр. Representational State Transfer — передача состояния представления) и повторная реализация интерфейса клиента на языках, поддерживаемых распространёнными браузерами (на данный момент это HTML5 (англ. аббр. HyperText Markup Language - язык для структурирования и представления) и CSS3 (англ. аббр. — Cascading Style Sheets — каскадные таблицы стилей)). После этих преобразований дальнейшая работа по совершенствованию системы заключается в изменении только той её части, которая всегда напрямую доступна на стороне сервера.

Предложенная система мониторинга позволяет оперативно отслеживать динамически изменяющиеся характеристики показаний окружающей среды на подконтрольном объекте, а также осуществлять контроль работы оборудования. Показания сенсоров и датчиков агрегируются в базе данных и по-

зволяют проводить анализ динамики различных характеристик среды. Информация о состоянии объекта может быть наглядно представлена пользователю в виде настраиваемых графиков и элементов управления, предыдущая реализация отображала показания через терминальный клиент[3,4]. Тестирование функционального макета происходило в течение пяти месяцев в различных промышленных помещениях и показало эффективность работы.

Было проведено маркетинговое исследование, которое выявило заинтересованность потенциальных потребителей в предложенном авторами проекте «Интегрируемая система мониторинга».

Примечания

1. 3 Reasons SCADA Software is Going Nowhere. // Ignition: One Platform, Unlimited Possibilites. URL: https://inductiveautomation.com/video/3-reasons-scada-going-nowhere (дата обращения: 24.12.2016).

2. Академия Microsoft: Лекция 1: Принципы работы и структура Web-приложений на основе ASP. NET. // «ИНТУИТ» национальный открытый университет. URL: http://www.intuit.ru/studies/courses/1139/250/lecture/6422 (дата обращения: 24.12.2016).

3. Зубов Я.М. Ильин И.И. Прототип системы удаленного мониторинга // Наука, образование, общество: актуальные вопросы и перспективы развития. -2015. - С. 65 - 66.

4. Зубов Я.М. Ильин И.И. Использование веб-технологий в Arduino - проекте для удаленного наблюдения за состоянием среды // Научные исследования в современном мире. -2015. - С. 36 - 38.

ИЛЬИН Иван Игоревич, студент кафедры «Безопасность информационных и автоматизированных систем» технологического факультета ФГБОУ ВО «Курганский государственный университет». 640020, г. Курган, ул. Советская, д. 63, стр.4. E-mail: wind069@gmail.com

ЗУБОВ Яков Михайлович, студент кафедры «Безопасность информационных и автоматизированных систем» технологического факультета ФГБОУ ВО «Курганский государственный университет». 640020, г. Курган, ул. Советская, д. 63, стр.4. E-mail: wind069@gmail.com

МОСКВИН Владимир Викторович, старший преподаватель кафедры «Безопасность информационных и автоматизированных систем» технологического факультета ФГБОУ ВО «Курганский государственный университет». 640020, г. Курган, ул. Советская, д. 63, стр.4. E-mail: bias.kgsu.techno@gmail.com

ПОЛЯКОВА Елена Николаевна, кандидат педагогических наук, заведующий кафедры «Безопасность информационных и автоматизированных систем» технологического факультета ФГБОУ ВО «Курганский государственный университет». 640020, г. Курган, ул. Советская, д. 63, стр.4. E-mail: penelena1972@yandex.ru

ILYIN Ivan, student of the Department of «Security of information and automated systems» of the faculty of technology of the «Kurgan state University». 640020, Kurgan, Sovetskaya street, 63, p. 4. E-mail: wind069@gmail.com

ZUBOV Iakov, student of the Department of «Security of information and automated systems» of the faculty of technology of the «Kurgan state University». 640020, Kurgan, Sovetskaya street, 63, p. 4. E-mail: wind069@gmail.com

MOSKVIN Vladimir Viktorovich, senior teacher of the Department «Security of information and automated systems» of the faculty of technology of the «Kurgan state University». 640020, Kurgan, Sovetskaya street, 63, p. 4. E-mail: bias.kgsu.techno@gmail.com

POLYAKOVA Elena Nikolayevna, the candidate of pedagogical Sciences, head of Department «Security of information and automated systems» of the faculty of technology of the «Kurgan state University». 640020, Kurgan, Sovetskaya street, 63, p. 4. E-mail: penelena1972@yandex.ru

Вестник УрФО № 4(22) / 2016, с. 38–43
УДК 341 : 004.056 + 327 : 004.056 + 004.056

Кузнецов П. У.

ОТДЕЛЬНЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В представленной статье анализируется формирование правового обеспечения международной информационной безопасности. Автор анализирует практический опыт американских экспертов Института Восток-Запад и российских ученых Института проблем информационной безопасности МГУ по разработке терминов в области информационной безопасности международного уровня.

Так же автором исследуются институциональные проблемы применимости традиционного международного права к сфере ИКТ, в частности проблема определения места специальных правовых инструментов в системе традиционных международных правовых средств.

В связи с этим, автор предлагает переосмыслить систему известных для правоведения средств, особенно таких, как: дозволения, запреты, обязывания, ограничения, сдерживания (удержания от совершения злоумышленных действий), связывания, предупреждение, стимулирование и др. Набор названных инструментальных правовых средств должен сбалансировано и гармонично определить контуры правового регулирования общественных отношений по поводу ИКТ на международном уровне.

Ключевые слова: *информация, информационная безопасность, информационно-коммуникационные технологии, информационное общество, информационное право, международная информационная безопасность, киберпространство.*

Kuznetsov P. U.

SOME ASPECTS OF FORMATION OF LEGAL ENSURING INTERNATIONAL INFORMATION SECURITY

In the present article on the basis of the formation of the legal analyzes of international information security. The author analyzes the experience of American experts at the EastWest Institute and the Moscow State Institute of Russian scientists in the field of the development of the terms of the international level of information security issues of information security.

As the author examines the institutional problems of the applicability of international law to the traditional field of ICT, in particular the problem of determining the place of specific legal instruments in the traditional international legal means.

In connection with this, the author proposes to rethink the system known for the Law of funds, especially such as: permission, bans, obliging, limitations, deterrence (deterring malicious acts), binding, prevention, promotion, etc. Set these tools remedies must. balanced and harmonious shape to the legal regulation of social relations on the ICT at the international level.

Keywords: *information, information security, information and communication technologies, information society, information law, the international information security, cyberspace.*

Известно, что защита интересов личности, общества и государства в информационной сфере (информационная безопасность) является одним из важных условий устойчивого развития глобального информационного общества.

Как справедливо подчеркивается в одном из последних докладов международной Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: «открытая, безопасная, стабильная, доступная и мирная ИКТ-среда имеет существенно важное значение для всех, но для ее создания необходимо эффективное сотрудничество между государствами в целях снижения угроз международному миру и безопасности».

Информационно-коммуникационные технологии (ИКТ) открывают широчайшие возможности преобразования экономики и культуры всех стран. Киберпространство является непременным атрибутом нашей повседневной жизни. ИКТ приносят колоссальную пользу движения к прогрессу. Однако они порождают и определенные риски. В последнее время наметились тревожные тенденции, которые создают угрозу реализации прогрессивных целей цифровой цивилизации, а также могут нанести ущерб международному миру и безопасности в целом[2]. Особенно сложная ситуация складывается с информационно-кибернетическим оружием, которое по своей мощи может быть приравнено к оружию массового поражения. По американским данным, 20-30 государств мира способны вести кибернетическую войну.[3]

Основным официальным документом, определяющим государственную политику РФ в области международной информационной безопасности является «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», утв. Президентом РФ 24.07.2013 (№ Пр-1753) [4]. Названный документ определил основной угрозой в области международной информационной безопасности – использование информационных и коммуникационных технологий:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы жизненно важной (критической) информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

К числу наиболее пагубных нападений с использованием ИКТ относятся нападения на критически важные объекты инфраструктуры и связанные с ними информационные системы государств. Опасность вредоносных нападений с использованием ИКТ на критически важную инфраструктуру является реальной и серьезной.

Существует все более реальная опасность использования ИКТ для террористических целей, в том числе для совершения террористических нападений на объекты ИКТ или связанную с ИКТ инфраструктуру, а не только для вер-

бовки сторонников, финансирования, обучения и подстрекательства, причем, если не принять соответствующих мер, то это может поставить под угрозу международный мир и безопасность.

Многообразие злонамеренных негосударственных субъектов (включая преступные группировки и террористов), их различные мотивы, быстротечность злонамеренных нападений в сфере ИКТ, а также трудности, связанные с определением источника инцидента в сфере ИКТ, увеличивают существующую угрозу. Государства с полным основанием обеспокоены опасностью дестабилизирующих последствий ошибочного понимания намерений другой стороны, потенциалом возникновения конфликта и возможностью нанесения ущерба их экономике.

Ряд государств наращивают потенциал в сфере ИКТ для военных целей. Использование ИКТ в будущих конфликтах между государствами становится более вероятным. Разный уровень развития потенциала обеспечения безопасности в сфере ИКТ между государствами может также привести к повышению уязвимости в условиях взаимосвязанного мира.

Существенно важное значение для борьбы с вызовами и угрозами в сфере международной информационной безопасности имеет эффективное сотрудничество между государствами. Обеспечение стабильности и безопасности в информационной сфере может быть достигнуто лишь по линии международного сотрудничества, причем основой такого сотрудничества должны являться нормы международного права и принципы, провозглашенные в Уставе Организации Объединенных Наций.

Одним из важных обстоятельств, препятствующих укреплению международной информационной безопасности, является отсутствие единой позиции по порядку применения норм и принципов международного права к регулированию международных отношений в этой сфере.

Поэтому весьма важным является проблема толкования принципов международного права, установленных Уставом ООН и Декларацией о принципах международного права 1970 г., применительно к ИКТ. Особенно таких принципов как принцип мирного разрешения споров, неприменение силы или угрозы силой, суверенного равенства государств, невмешательства, равноправие и самоопределение народов, добросовестного выполнения обязательств по международному праву и принцип сотрудничества.

Как правильно подчеркивает А.А. Стрельцов, сложность решения проблемы применения международного права безопасности к киберпространству обусловлена следующими основными факторами:

• отсутствие согласия между государствами- членами ООН по многим вопросам правового регулирования;

• процессы злонамеренного использования ИКТ трудно фиксировать. Вследствие этого невозможно без использования специальных технических средств объективно установить ни факты вредоносного использования ИКТ, ни последствия такого использования ИКТ (величина и виды ущерба), ни субъектов, осуществляющих эти деяния. Общепринятые признаки вредоносного использования ИКТ, подлежащие регистрации техническими средствами, международным сообществом не определены. Международная система объективизации событий и идентификации субъектов в киберпространстве отсутствует;

• международными документами средства ИКТ не обладают признаками традиционного оружия. Это существенно затрудняет классификацию применения ИКТ в качестве «вооруженного нападения» или «вооруженных действий», порождающих, соответственно, правоотношения, связанные как с применением права на самооборону, так и с соблюдением норм международного гуманитарного права;

• правоприменение в области международной информационной безопасности осуществляется государствами самостоятельно с использованием национальных или региональных систем технических средств объективизации событий и атрибуции субъектов. В рамках юрисдикции одного государства или группы дружественных государств правоприменение базируется на презумпции добросовестности действий лиц, осуществляющих оперативно следственные мероприятия по фактам злонамеренного использования ИКТ. При взаимодействии государств, не связанных отношениями доверия, презумпция добросовестности невозможна ввиду того, что технологический потенциал многих государств достаточен для того, чтобы фальсифицировать данные о почти любых событиях и субъектах киберпространства;

• в международном праве отсутствуют механизмы закрепления адресного про-

странства применения ИКТ к национальным границам. В настоящее время функции распределения IP-адресов выполняются в основном негосударственными организациями, не являющимися субъектами международных публичных отношений. Это создает дополнительные сложности при определении в киберпространстве границ театров военных действий, нейтральных государств, обозначении объектов и лиц, охраняемых международным публичным правом;

• учитывая, что ни одно государство не имеет международных обязательств в области обеспечения безопасности киберпространства, представляется затруднительным определение границ национального суверенитета и юрисдикции государств. Данный вопрос особенно важен в свете существующей практики государств рассматривать обеспечение безопасности киберпространства в качестве одной из составляющих национальной безопасности.[5]

Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по формированию системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях, являются:

а) создание условий для продвижения на международной арене российской инициативы в необходимости разработки и принятия государствами - членами ООН Конвенции об обеспечении международной информационной безопасности;

б) содействие закреплению российских инициатив в области формирования системы международной информационной безопасности в итоговых документах, изданных по результатам работы Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также содействие выработке под эгидой ООН правил поведения в области обеспечения международной информационной безопасности, отвечающих национальным интересам Российской Федерации;

в) проведение на регулярной основе двусторонних и многосторонних экспертных консультаций, согласование позиций и планов действий с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности, государствами - участниками БРИКС, странами - членами Азиатско-тихоокеанского экономического сотрудничества, другими государствами и международными структурами в области международной информационной безопасности;

г) продвижение на международной арене российской инициативы в интернационализации управления информационно-телекоммуникационной сетью «Интернет»;

ж) создание условий для заключения между Российской Федерацией и иностранными государствами международных договоров о сотрудничестве в области обеспечения международной информационной безопасности;

и) использование научного, исследовательского и экспертного потенциала ООН, других международных организаций для продвижения российских инициатив в области формирования системы международной информационной безопасности

Одним из важных традиционных международно-правовых средств является укрепление доверия. Меры укрепления доверия способствуют поддержанию международного мира и безопасности. Они могут способствовать расширению межгосударственного сотрудничества, повышению степени транспарентности, предсказуемости и стабильности. В стремлении укрепить доверие, в целях создания мирной ИКТ-среды, государства должны принимать во внимание Руководящие принципы для мер по укреплению доверия, принятые Комиссией по разоружению в 1988 году и утвержденные консенсусом Генеральной Ассамблеей в резолюции 43/78 (H). В целях укрепления доверия и расширения сотрудничества возможно создание системы проведения двусторонних, региональных, субрегиональных и многосторонних консультаций в целях снижения риска ошибочного восприятия, эскалации конфликтов, которые могут быть вызваны инцидентами в сфере ИКТ.

Это может включать добровольное распространение национальных мнений и информации:

• о различных аспектах национальных и транснациональных угроз ИКТ и в сфере использования ИКТ;

• факторах уязвимости и установленных пагубных скрытых функций в продуктах ИКТ;

• передовых методах обеспечения безопасности ИКТ;

• мерах укрепления доверия, разработанных в рамках региональных и многосторонних форумов;

• распространении опыта деятельности национальных организаций, политике и программах, имеющих отношение к безопасности ИКТ;

• национальных законах и стратегиях обеспечения безопасности критически важных объектах инфраструктуры ИКТ.

Государства должны стремиться укреплять трансграничное сотрудничество в устранении транснациональных факторов уязвимости критически важной инфраструктуры ИКТ. Такие меры могут включать создание двусторонних, субрегиональных, региональных и многосторонних основ технических, правовых и дипломатических механизмов укрепления доверия в и предупреждения инцидентов в сфере ИКТ. Ярким примером международного сотрудничества в области информационной безопасности является «Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности», заключенное в г. Екатеринбурге 16.06.2009, которое 2 июня 2011 года вступило в силу.

Странам-членам Шанхайской организации сотрудничества (ШОС) удалось добиться реального прорыва в продвижении идеи формирования международной системы обеспечения международной информационной безопасности (МИБ). Идея и конкретный проект этого соглашения были предложены российской стороной. Соглашение отвечает принципам и задачам деятельности ШОС, предусматривающим координацию действий, оказание взаимной поддержки и налаживание тесного сотрудничества по важнейшим международным и региональным вопросам, к которым, в частности, относится и проблематика обеспечения МИБ.

Уникальность названного документа заключается в том, что он впервые в международно-правовом плане определяет наличие и существо конкретных угроз в области МИБ, а также основные направления, принципы, формы и механизмы сотрудничества сторон в этой сфере. Как в рамках ШОС, так и в международной практике, вступившее в силу Соглашение стало первым договорным актом, направленным на ограничение всего комплекса угроз МИБ, включая их военно-политические, криминальные и террористические аспекты. Вступившее в силу Соглашение отвечает идее и цели создания всеобъемлющей системы обеспечения международной информационной безопасности.

Мировое сообщество по обеспечению информационной безопасности стоит на пороге формирования нового направления в системе правового регулирования – международного права информационной безопасности. В традиционных рамках международного права безопасности и вооруженных конфликтов[6] уже невозможно удерживать новую ИКТ-среду, особенно стихию использования сети Интернет. Поэтому следует говорить не столько о кризисе международного права, сколько о создании его нового формата (международного права 2.0) в контексте безопасности глобального информационного общества**.**

Очевидно, что новые киберобъекты формируют новый класс общественных отношений, возникающих по поводу ИКТ (информационно-коммуникационных технологий) в названной новой киберсферы. Мы переживаем время включения таких объектов отношений в сферу правоотношений, т.е. правовое пространство. Процесс этот сложный, болезненный и достаточно длительный (он длится уже более 25 лет), с момента принятия первых нормативных правовых актов информационной тематики, в т.ч. включения норм права об использовании информационных систем в различные отрасли права.

Как известно, для того, чтобы включить любой технологически сложный объект жизни в правовую сферу, требуется с помощью средств логики и лингвистики подвергнуть их комплексному исследованию с позиций разных научных специальностей.

В первую очередь необходимо когнитивно обработать термины, обозначающие границы технически сложных объектов (выявить и понять их технологические признаки, имеющие правовое значение).

Во-вторых, необходимо все существенные понятийные признаки и черты с помощью юридической техники преобразовать в правовые свойства и значения, т.е. технически сложные слова и словообразования привести в удобную для правоведов форму.

В-третьих, на основе правовых признаков и значений названных сложных терминов необходимо сформулировать определение (дефиницию), т.е. подготовить такие термины для включения их в состав модели правового поведения, т.е. в норму права.

Долгое время в науке отсутствовал набор признаваемых основных терминов и их зна-

чений, предназначенных для использования в нормативных документах международного уровня по вопросам информационной безопасности.

В 2011 году совместными усилиями американских экспертов Института Восток-Запад и российских ученых Института проблем информационной безопасности МГУ был достигнут консенсус по терминологии в трех ключевых областях кибербезопасности. Была создана концептуальная основа для обеспечения процесса создания определений для общего международного словаря как необходимого этапа выработки «Правил дорожного движения». Речь идет о двустороннем проекте Россия-США по выработке основ критически важной терминологии в области кибербезопасности. [7] Названным проектом разработаны первые двадцать терминов в области информационной безопасности международного уровня. Авторы этого проекта считают, что они создали основу, опираясь на которую можно работать дальше – как в двустороннем формате между нашими странами, так и в многостороннемс аспекте.

Думается это действительно так, хотя внимательный анализ названного проекта позволяет сделать вывод о том, что каждый из названных терминов и их определений необходимо подвергнуть правовому осмыслению, поскольку предлагаемые их значения могут «пробуксовывать» в ходе их применения в правоприменительной практике.

Не менее важным аспектом являются институциональные проблемы применимости традиционного международного права к сфере ИКТ. Речь идет об определении места специальных правовых инструментов в системе традиционных международных правовых средств.

Здесь необходимо переосмыслить систему известных для правоведения средств, особенно таких, как: дозволения, запреты, обвязывания, ограничения, сдерживания (удержания от совершения злоумышленных действий), связывания, предупреждение, стимулирование и др. Набор названных инструментальных правовых средств являются правовыми конструкциями первого уровня, которые с помощью сочетания жестких и мягких режимами должны сбалансировано и гармонично определить контуры правового регулирования общественных отношений по поводу ИКТ на международном уровне.

Примечания

1. Семидесятая сессия Генеральной Ассамблеи ООН открылась 15 сентября 2015 года в 15.00 в Центральных учреждениях ООН в Нью-Йорке // Генеральная Ассамблея ООН. URL: http://www.un.org/ru/ga/70 (дата обращения: 08.09.2016).

2. Бирюков А. В. Современные международные научно-технологические отношения: монография. М., 2014. С. 100 – 104.

3. Бирюков А. В. Указ.соч. С.100.

4. Совет безопасности Российской Федерации // Совет безопасности Российской Федерации. Официальный сайт. URL:http://www.scrf.gov.ru/ (дата обращения: 08.09.2016).

5. Стрельцов А. А. Проблемы адаптации международного права к информационным конфликтам // Труды Седьмого международного научного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» и Седьмая научная конференция Международного исследовательского консорциума информационной безопасности 22-25 апреля 2013 года г.Гармиш-Партенкирхен, Германия». М. 2013. С. 124-128.

6. Международное право. Учебник для вузов. Отв. редакторы – проф. Г.В.Игнатенко и проф. О.И.Тиунов. М., 1999. С. 431 – 464.

7. Двусторонний проект: Основы критически важной терминологии // Института проблем информационной безопасности МГУ. Официальный сайт. URL:http://www.iisi.msu.ru/articles/article36/ (дата обращения: 08.09.2016).

Кузнецов Петр Уварович, заведующий кафедрой информационного права Уральского государственного юридического университета, доктор юридических наук, профессор. Россия, 620066, г. Екатеринбург, ул. Комсомольская. E-mail: petr_kuznecov@mail.ru

Kuznetsov Petr Uvarovich, Head of Information Law department Ural State Law University, Doctor of Jurisprudence, Professor. Russia, 620066, Ekaterinburg, Komsomolskaya street, 21. E-mail: petr_kuznecov@mail.ru

Вестник УрФО № 4(22) / 2016, с. 44–48
УДК 342.922/951 : 354 342.9 : 004.056 + 354 : 004.056

Ковалева Н. Н.

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

В статье раскрываются отдельные проблемы информационной безопасности при использовании информационных технологий в государственном управлении. Для решения проблем информационной безопасности при использовании информационных технологий в государственном управлении необходимо интегрировать усилия на различных уровнях управления: федеральном, субъектов федерации и муниципальном. Для реализации общей координации разрешения проблем в сфере обеспечения информационной безопасности предлагается создать Научно-технический совет по проблемам информационной безопасности при высшем органе исполнительной власти субъекта Федерации, который определял бы специфические подходы и методы решения. В то же время сеть координационных советов при наиболее компетентных предприятиях, учреждениях и организациях субъекта Федерации могла бы обеспечивать решение конкретных организационно-технических вопросов.

Ключевые слова: *информационная безопасноть, использование информационных технологий, государственное управление, взаимодействие государственных и мциципальных органов.*

Kovaleva N. N.

THE ORGANIZATIONAL AND LEGAL ISSUES OF INFORMATION SECURITY IN THE RUSSIAN FEDERATION

The article describes the individual information security problems in the use of information technologies in public administration. To solve information security problems in the use of information technologies in public administration need to integrate efforts at the various levels of government: federal, federal subjects and municipal. To implement the overall coordination to solve problems in the field of information security is proposed to establish scientific and technical advice on issues of information security at the highest executive authority of the Federation, which would define specific approaches and methods of solution. At the same time coordinating councils with the most competent network of enterprises, institutions and organizations of the Federation could provide a solution to specific organizational and technical issues.

Keywords: *information security, use of information technology, public administration, the interaction of state and municipal authorities*

По прогнозам ученых, со второй половины XXI века технические и технологические процессы повлекут за собой радикальную трансформацию политической картины мира, что изменит распределение ролей среди государств.

Государство же в становлении информационного общества играет роль координатора деятельности различных субъектов общества, способствует интеграции людей в информационно-техническое окружение. По мнению Э. Тоффлера[1], тенденция к всеобщей унификации породила свою противоположность – стремление к разнообразию и индивидуальности, которые в большей степени отвечают психологической природе человека. Само появление и функционирование «всемирной паутины» связывается с одной стороны с общими мировыми тенденциями демократизации общественных и межгосударственных отношений, а с другой – с глобализационными процессами.

Стремительное развитие и внедрение новейших информационных технологий во все сферы жизнедеятельности является несомненным благом, открывающим возможности для экономического роста, повышения общественного благосостояния. Однако следует помнить и об угрозах, о возможных негативных последствиях, к которым могут привести научные, информационные и коммуникационные достижения

В ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»[2] было предусмотрено, что для координации внедрения мероприятий по управлению информационной безопасностью в большой организации необходимо создать комитет.

Если рассмотреть функции данного комитета и применить их расширительно к государственному уровню, то можно определить, что данная структура на уровне государства должна включать представителей министреств и ведомств и заниматься выполнением следующих направлений деятельности:

• согласовывать конкретные функции и обязанности в области информационной безопасности на уровне государства;

• согласовывать конкретные методики и процедуры информационной безопасности, например, такие как оценка рисков, классификация информации с точки зрения требований безопасности;

• согласовывать и обеспечивать поддержку инициатив и проектов в области информационной безопасности на оровне государства, например, таких как разработка программы повышения квалификации государственных служащих в области безопасности;

• обеспечивать учет включения требований безопасности во все проекты, связанные с обработкой и использованием информации;

• оценивать адекватность и координировать внедрение конкретных мероприятий по управлению информационной безопасностью для новых систем или услуг;

• проводить анализ инцидентов нарушения информационной безопасности;

• способствовать демонстрации поддержки информационной безопасности со стороны высшего руководства страны.

Так, Мигачев Ю. И., Молчанов Н. А.[3] предлагают необходимым в Федеральном законе «О безопасности» и Стратегии национальной безопасности Российской Федерации до 2020 года сформулировать основные направления деятельности государственных органов безопасности по обеспечению информационной безопасности. Однако, представляется целесообразным разработка новой Доктрины информационной безопасности, более структурного и развернутого документа, который бы содержал соотвествующие направления деятельности для государственных органов. К тому же работа над этим документом в настоящее время активно ведется. О чем в частности свидетельствует проведение Международной научной конференции по информационному праву и информационной безопасности на тему: «Новые вызовы и угрозы информационной безопасности: правовые проблемы» Институтом государства и права РАН 5-6 февраля 2016 года[4].

Если учесть, что одной из краеугольных проблем при осуществлении информационного обеспечения является недостаточность взаимодействия органов власти различных ведомств и уровней, то отсюда следует, что в целях повышения эффективности технологий электронного государства необходимо реформировать систему государственного управления информационным обеспечением в России. Ряд шагов в этом направлении уже сделан. Так, Постановление Правительства РФ от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия» (в ред. постановлений Правительства РФ от 8 июня 2011 г. № 451, от 28 ноября

2011 г. № 977) устанавливает, что Минкомсвязи России обладает полномочиями государственного заказчика и оператора по отношению к единой системе межведомственного электронного взаимодействия, а также координирует деятельность по подключению к этой системе. Однако этого недостаточно, так как анализ действующей системы органов власти, реализующих государственное управление информационным обеспечением в Российской Федерации, показывает отсутствие четко выстроенной и взаимоувязанной иерархии в этой сфере. Думается целесообразно придать Роскомнадзору статус относительно независимого федерального органа исполнительной власти — федеральной службы при Правительстве РФ с подчиненными ему структурами на уровне субъектов Федерации и на местном уровне. При этом данный орган власти должен обеспечивать создание единого информационного пространства не только с точки зрения его технического, но и сущностного наполнения, а также распределения финансовых потоков на выполнение данной задачи. Одновременно в его функции включается решение задач в области информационной безопасности и защиты личной жизни. В свою очередь в каждом органе исполнительной власти, как федеральном, так и на уровне субъектов Федерации и на местном, предполагается обязательное введение должности – ответственного за внедрение информационных технологий в деятельность органов исполнительной власти и контроль за их реализацией, который назначается по согласованию с создаваемой структурой. Представляется особенно важным объединение функций контроля и надзора в сфере защиты информации с контролем за финансированием этих процессов.

Это будет способствовать более тесному взаимодействию органов власти и граждан по предметно-функциональному признаку, а также персонализации ответственности при организации информационного взаимодействия.

Кроме того, данный подход даст возможность решить одну из основных задач процесса внедрения информационно-коммуникационных технологий в сферу публичного управления: повысить эффективность деятельности государственных и муниципальных органов, что, в свою очередь, обеспечит более эффективную реализацию права на доступ к информации и предоставление государственных и муниципальных услуг гражданам России на более качественном уровне[5].

Следует указать, что необходимо реализовывать информационное взаимодействие, координировать органы исполнительной власти субъекта Федерации и федеральные территориальные органы исполнительной власти, хозяйствующие субъекты, которые организационно образуют названную информационную систему субъекта Федерации. Д.Л. Абрамович предлагает наделить подобную структуру, кроме названных, следующими функциями:

• формировать и проводить в субъекте Федерации стратегию информационного обеспечения, которая учитывает как интересы органов исполнительной власти, так и всех других участников информационной сети;

• сформулировать принципы унификации используемых информационных технологий и требований объединения государственного и информационного ресурса с иными;

• обеспечивать информационную безопасность, регламентировать доступ к информационному ресурсу;

• разрабатывать общие критерии соответствия, регламенты представления, формы, протоколы и иные формализованные требования к сведениям, которые размещаются в информационной сети для открытого доступа;

• обеспечить административно-правовое регулирование деятельности информационной системы.[6]

Следует отметить, что на территории субъекта Федерации осуществляют свою деятельность федеральные органы исполнительной власти и органы исполнительной власти субъекта РФ. Между ними существует активное информационное взаимодействие, которое выражается в координации информационной деятельности, создании информационного ресурса общего пользования, обеспечении информационной безопасности, осуществлении информационного обмена. Для решения основной задачи управления информационным обеспечением на уровне субъекта Федерации необходимо оптимизировать информационные связи, усилия и затраты в целях обеспечения представления информации федеральным органам[7].

Внедрение информационно-коммуникационных технологий позволяет соответствующим службам непосредственно создавать и сопровождать лишь необходимые для их непосредственной деятельности информационный ресурс, а к другим источникам информа-

ции организовывать доступ в режиме реального времени. При этом происходит большое количество информационных контактов, которые могут быть открытыми и закрытыми. Открытые – контакты, информационные службы или другие структуры, гарантирующие информационную безопасность необеспечиваемым регламентируемым доступом. В основном такой доступ реализуется с использованием информационных сетей типа Интернет. В свою очередь, закрытые информационные контакты реализуются внутри локальных информационных сетей органов исполнительной власти субъектов Федерации и муниципальных образований, они изолированы от сетей типа Интернет или осуществляются через специальные каналы передачи данных. Ошибочно считать, что такое разграничение доступа на уровне органов исполнительной власти субъектов Федерации и муниципальных образований является лишней перестраховкой, что информационный ресурс органов исполнительной власти субъектов Федерации и муниципальных образований не представляет интереса. Так, в открытой информации могут подтверждаться или опровергаться какие-либо закрытые сведения; содержаться персональные данные, которые обеспечат работу в отношении какого-либо конкретного субъекта и т.п.[8]

Кроме того, иностранные разведки или местные преступные элементы могут быть заинтересованы в сведениях, которые содержатся в интегрированных в общую сеть государственных и муниципальных реестров, регистров, кадастров.

Способствовать обеспечению информационной безопасности также призвана межведомственная интегрированная автоматизированная система контроля пропуска через государственную границу, которая повышает эффективность деятельности пограничных органов и сокращает время, необходимое для прохождения через пункты пропуска; обеспечивает интересы и безопасность нашего государства, в связи с тем, что противодействует проникновению на территорию России международного терроризма, международной преступности и др. Кроме того, государственная автоматизированная система подготовки паспортов и виз нового поколения позволит предотвратить незаконную миграцию, исключив фальсификацию или незаконное использование паспортно-визовых документов; повысит эффективность контроля при пересечении границ и защиту от подделки документов, удостоверяющих личность; обеспечит техническую возможность обмена информацией с другими государствами в целях искоренения незаконной миграции, криминальных и террористических проявлений. [9].

В то же время информационное обеспечение государственных и муниципальных органов исполнительной власти возможно только при условии обеспечения достаточного уровня информационной безопасности.

Анализ деятельности информационных служб привел к появлению комплекса проблем, затрудняющих дальнейшее развитие, к которым относятся следующие:

• установление и применение административной и дисциплинарной ответственности лиц, представляющих информацию, за полноту, достоверность, актуальность информационного ресурса;

• нормативное закрепление административно-правовых режимов, административных регламентов обмена информацией внутри органов государственного и муниципального управления;

• установление административно-правового положения, нормативного порядка платного предоставления государственных и муниципальных ресурсов;

• контроль и надзор за реализацией общих стандартов и технических протоколов функционирования внутриведомственных информационных систем.

В связи с тем, что информационные системы и сети активно внедряемые органами исполнительной власти субъектов Федерации и муниципальных образований, часто создавались независимо друг от друга, необходимо координировать их дальнейшее развитие и использование как элементов единого государственного информационного пространства.

Однако в качестве пилотного проекта в Татищевском районе Саратовской области уже с 2011 года активно внедряется предоставление государственных и муниципальных услуг в электронном виде на основе межведомственного взаимодействия [10].

Для того чтобы обеспечить жизнедеятельность субъектов РФ и муниципальных образований и их органов исполнительной власти комплексной, оперативной, полной и актуальной информацией, необходимо в ходе совершенствования информационного обеспечения государственных и муниципальных орга-

нов провести внутритерриториальную интеграцию и оптимизацию информационного ресурса соответствующих территорий независимо от формы собственности. Информационная безопасность субъекта Федерации и (или) муниципального образования является одним из существенных факторов, обеспечивающих эффективное социально-экономическое развитие соответствующих территорий. Под информационной безопасностью часто понимают состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних угроз в условиях использования информационных технологий. При этом реализация мер информационной безопасности позволяет должным образом обеспечить права субъектов права на достоверную информацию, получаемую законным способом, защищать разного рода конфиденциальную информацию, сохранять и приумножать культурные и духовно-нравственные ценности, исторические традиции и нормы общественной жизни [11].

Системы информационной безопасности в настоящее время активно создаются в субъектах Федерации, однако включение в эту систему муниципальных образований пока идет недостаточно активно и представляет одно из перспективных направлений развития систем информационной безопасности в России.

Примечания

1. См.: Тоффлер Э. Третья волна. – М.: АСТ, 1998

2. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью // http://gostexpert.ru/gost/gost-17799-2005 (дата обращения 22.04.2016)

3. Мигачев Ю.И., Молчанов Н.А. Правовые основы национальной безопасности (административные и информационные аспекты)// http://отрасли-права.рф/article/7087 (дата обращения 22.04.2016)

4. Международная научная конференция по информационному праву и информационной безопасности на тему: «Новые вызовы и угрозы информационной безопасности: правовые проблемы»// http://www.igpran.ru/nlive/3932/ (дата обращения 13.05.2016)

5. Ковалева Н. Н. Административно-правовое регулирование использования информационных технологий в государственном управлении /Диссертация на соискание ученой степени доктора юридических наук. -Саратов, 2014.С.194-195

6. Абрамович Д.Л. Информационное обеспечение муниципального управления. Сыктывкар, 2007. С.108

7. Ковалева Н. Н. Там же. С.228-229.

8. Федотова Е.Л. Информационные технологии и системы. М., 2009. С.49

9. Государственная программа Российской Федерации «Информационное общество (2011–2020 годы)»: утверждена распоряжением Правительства РФ от 20 октября 2010 г. № 1815-р // Собр. законодательства Рос. Федерации. 2010. № 46, ст. 6026; 2012. № 4, ст. 514.

10. Постановление Администрации Татищевского муниципального района Саратовской области от 21 декабря 2011 г. № 1402 «Об организации предоставления государственных и муниципальных услуг», а также Постановление Администрации Татищевского муниципального района Саратовской области от 22 февраля 2012 г. № 313 «О внесении изменений в постановление Администрации Татищевского муниципального района Саратовской области от 21 декабря 2011 г. № 1402». URL: http://tatishevo.saratov.gov.ru/ (дата обращения: 01.05.2012).

11. Васильев А.А. Система муниципального управления. М., 2010. С. 114

КОВАЛЕВА Наталия Николаевна, профессор кафедры административного и муниципального права федерального государственного бюджетного образовательного учреждения высшего образования «Саратовская государственная юридическая академия», доктор юридических наук, доцент. 410056, г.Саратов, ул. Вольская, д.1. E-mail: kovaleva.natalia@mail.ru

KOVALEVA Natalia, a professor of the Department of Administrative and Municipal Law of the Federal State Budgetary Educational Institution of Higher Education «Saratov State Academy of Law», Doctor of Law, docent. 410056, Saratov, ul. Volsky, 1. E-mail: kovaleva.natalia@mail.ru

УДК 004.056 + 347.961.38 + 34:002 Вестник УрФО № 4(22) / 2016, с. 49–54

Паршуков М. И.

ТАЙНА КАК ПРАВОВАЯ КАТЕГОРИЯ

В представленной статье анализируется институт тайны в праве, исследуется его природа, анализируются признаки тайны, делается вывод о тайне как базовой правовой категории информационного права.

Институт тайны является важнейшим, системообразующим средством обеспечения информационной безопасности. Несмотря на это, единообразного подхода к определению понятия тайны и его места в общей системе понятийного аппарата нет даже в рамках одной науки информационного права. Так, тайна определяется как правовой режим или как конфиденциальные сведения.

Право, использующее некорректные определения не будет исполнимым, непоследовательность законодателя в вопросе правового определения тайны уже сегодня ведет к ошибкам практике правового регулирования.

Тайна является в силу своей уникальной природы общеправовой категорией, используемой всеми отраслями права, что находит свое отражение в десятках законодательных актах, в свою очередь вводящих в правовой оборот различные виды информации, охраняемые в режиме тайны.

Ключевые слова: *информация, информационная безопасность, информационное право, конфиденциальные сведения, понятийный аппарат, правовой режим, тайна.*

Parshukov M. I.

SECRET AS LEGAL CATEGORY

In the present article on the basis of analyzes Institute of secrecy law, his nature is studied, analyzed signs secrets, concludes a secret basic legal categories of information law.

The institute of secret is the most important, backbone instrument for ensuring of information security. Despite it, there is no uniform approach to definition of concept of secret and his place in the general system of a conceptual framework even within one science of information right. So, the secret is defined as a legal regime or as a confidential information.

Generally used incorrect determination will not be enforceable, the inconsistency of the legislator in the issue of the legal definition of the mysteries of today leads to errors regulatory practice.

The secret is owing to the unique nature the all-legal category used by all branches of the right that finds the reflection in tens the acts in turn introducing the different types of information protected in the secret mode into legal circulation.

Keywords: *information, information security, information law, confidential information, conceptual apparatus, the legal regime, secret.*

Тайна всегда сопровождала человека на всем его историческом пути развития. Все сокрытое, неизвестное, неведомое и сокровенное является смыслом тайны и всегда составляло часть жизненной действительности и инструментом выживания.[1] Институт тайны является важнейшим, системообразующим средством обеспечения информационной безопасности. Несмотря на это, единообразного подхода к определению понятия тайны и его места в общей системе понятийного аппарата нет даже в рамках одной науки информационного права.

Начиная исследование, уместно подвергнуть природу тайны лингвистическому анализу. В русском языке слово «тайна» имеет глубокие корни, оно древнерусского происхождения и первоначально употреблялось в мужском роде – «тай».[2] Слово «тайна» происходит от старославянского слова «тайбъна» и «тайбъно»; отсюда употреблялись названия «таибница» или «особая комната для занятий, не для гостей», а также «таинник» или «наперсник, любимец царя, вельможи, доверенный, негласный советник».[3]

В. И. Даль трактует слово «таить» как «таивать что, скрывать от других, содержать в скрытности, в неведении от кого-либо, в сокровенности, хоронить; не говорить чего, не сказывать, не показывать; отпираться, запираться, лгать».[4] Аналогичное объяснение слова «тайна» можно найти и в «Толковом словаре русского языка» С. И. Ожегова и Н. Ю. Шведовой. Понятие «тайна» рассматривается в трех смыслах: 1. Нечто неразгаданное, еще непознанное; 2. Нечто скрываемое от других, известное не всем, секрет; 3. Скрытая причина чего-нибудь.[5]

В толковом словаре Д. Н. Ушакова тайна раскрывается как: 1. то, что неизвестно, не стало еще доступным познанию, нечто непонятное, неразгаданное; 2. то, что скрывается от других, что известно не всем, секрет.[6]

Т. Ф. Ефремова придает слову «тайна» следующие значения: 1. то, что намеренно скрывается от других; секрет; 2. то, что еще не известно, не стало доступным познанию; 3. то же, что: таинство. Слову «таить»: держать в тайне (1), скрывать от других; хранить в себе, скрывать (чувства, мысли и т.п.) (2); заключать в себе что-либо незаметное или еще не проявившееся, сохранять, удерживать (3).[7]

Кроме того, в словаре Т. Ф. Ефремовой дается толкование слов «таинственный», «таиться», «тайноведец», «тайновидец» через смысловое содержание данных слов также раскрывается природа тайны. Прилагательное «таинственный» имеет следующие значения: «1. Соотносящийся по знач. с сущ.: тайна, связанный с ним. 2. Заключающий в себе тайну (1). 3. Окруженный тайной (2), преисполненный тайны, загадочный, непонятный. 4. Стоящий за пределами человеческого понимания; непостижимый.[8] Глагол «таиться» - прятаться, скрываться; существовать в скрытом виде, быть едва заметным; проявлять скрытность».[9] Существительное «тайноведец» - «Тот, кому доверены тайны, кто участвует в ведении секретных дел», а также «тайновидец» - «Тот, кто способен проникнуть в тайны, не доступные другим».[10]

Подводя итог краткому лингвистическому анализу, следует согласиться с мнением А. А. Фатьянова, отмечающего, что русским языком точно определены основные аспекты понятия тайна и основные сферы человеческих действий, которые за ним стоят: с одной стороны, это все то, что на данный момент не познано человеческим интеллектом, с другой - это сведения, с определенной целью сокрытые от других людей.[11] А. А. Фатьянов приходит к выводу, что тайна - это сфера объективной реальности, скрытая от нашего восприятия либо понимания.[12]

Говоря о природе тайне, заслуживает внимание исследование мнения дореволюционного правоведа В. В. Розенберга, утверждающего что, хотя жизнь в обществе и общение с другими людьми и составляет естественный удел каждого человека, однако, далеко не все отношения индивида являются общественным достоянием, доступны глазу и уху нашего ближнего. Каждый человек создает себе более или менее широкую сферу интимных отношений, которую он старается, по возможности, тщательно охранить от проникновения в нее третьих лиц, движимых к тому любопытством или какими-либо иными побуждениями. В свою очередь самые разнообразные мотивы заставляют людей охранять от третьих лиц те или другие свои отношения и окутывать их покровом тайны – в качестве психических факторов здесь можно встретить всю бесконечную скалу причин наших действий – от почти инстинктивного чувства стыдливости до соображений чисто материального свойства. Третьи лица стремятся насильственно проникнуть в эти тайны, сорвать завесу, разрушить секрет.[13]

Природа тайны может быть осмыслена через понимание ее как основного инстру-

мента выживания в агрессивном, постоянно меняющемся мире.

Институт тайны исторически призван был защищать жизненноважную информацию человека во всех сферах его деятельности с целью обеспечения своего существования.

В научных источниках мы находим и теоретический анализ природы тайны как явления. По мнению П. У. Кузнецова, главным характеризующим признаком информации, составляющей тайну, являются ее признаки, маскирующие существо отдельной событийной жизни от третьих лиц, степень конфиденциальности информации как «маскирующее» состояние зависит от ее характера и значения для общества. [14]

Природу тайны П. У. Кузнецов раскрывает, основываясь на теории отражения информации. Так, по его мнению, назначение тайны заключается в том, чтобы создать в структуре модели информации условия или некие преграды, ограничивающие коммуникативные процессы движения сигнала (сообщения) от коммуникатора (событий существующей действительности) к получателю (образы этой действительности). В обычной коммуникативной среде (информационном обмене) сигнал, естественно, должен достигнуть его получателя и отразиться в мыслительном образе в форме сведений. В структуре конфиденциальной информации сигнал как адекватное отражение о фактах и событиях жизненной действительности, подлежащей «маскировке», искусственно ограничивается при дальнейшей передаче его к пользователям. Таким образом, такой сигнал (сообщение) конфиденциального (тайного) характера не находит дальнейшего движения к получателю и не распространяется. Механизм формирования своеобразной «маскировки», то есть его искусственного ограничения для восприятия становится самостоятельной сферой человеческой деятельности, связанной непосредственно с информацией, а не с объектами событийной действительности, которые отражаются в информации. [15]

По мнению И. Л. Бачило, в российской правовой науке пока нет единого понимания тайн и их места в правовой системе. Существуют два основных подхода: тайна может пониматься как сведения, доступ к которым ограничен (М. А. Вус, А. А. Фатьянов), т.е. объект правовых отношений, или как правовой режим тех же сведений (О. А. Городов). [16]

Не было единого понимания тайны и в дореволюционной, и советской правовой науке.

Л. Е. Владимиров называл тайною сохранение в негласности обстоятельства, разглашение которого принесло бы больше вреда, чем пользы, понимая последнюю не только в смысле утилитарном, но и в смысле отвлеченном, т. е. как ограждение существования и питания нравственных идеалов человеческого совершенствования. [17]

Л. О. Красавчикова в монографическом исследовании, посвященном правовой защите личной жизни, указывала на то, что тайна - определенная информация о действиях (состоянии и иных обстоятельствах) определенного лица (гражданина, организации, государства), не подлежащая разглашению. [18]

Подробнее хотелось бы остановиться на анализе научного подхода О. А. Городова к пониманию тайны.

Им сделан вывод о том, что законодатель рассматривает тайну в широком смысле в качестве объективно существующих, но неизвестных третьим лицам сведений о чем-либо.

О. А. Городов считает, что если рассматривать информацию как знание, как меру устранения неопределенности представления о чем-либо, то тайные сведения являются информацией только для лиц, имеющих к ним доступ. Следовательно, неизвестность (незнание) это не информация, а нечто ей противоположное. В теории информации это нечто обозначается как мера неопределенности сведений и именуется энтропией. Таким образом, тайна выступает в качестве информации только для обладателя последней, но для третьих лиц до момента получения соответствующих сведений такая тайна будет выступать в качестве «энтропии». Закрытая информация для ее обладателя не тайна, но и для третьих лиц не информация. В этом проявляется двойственный, полярный характер тайны, который обусловлен наличием механизма доступа к сведениям, основанного на запретах и позитивных обязываниях, устанавливаемых законодателем в отношении третьих лиц и обладателей закрытых сведений соответственно. Основываясь на этом, О. А. Городов приходит к выводу, что тайна - правовой режим информации. [19]

К аналогичному выводу приходят в совместной монографии М. В. Пермяков и Э. Ф. Шамсумовна, утверждающие что тайна есть все таки правовой режим, то есть, во-первых, закрепленное правовыми нормами и обеспе-

ченное совокупностью юридических средств комплексное системообразующее установление порядка информации, доступ к которой ограничен; во-вторых, тайна в праве отражает реально существующие общественные отношения и уровень развития правовой системы в целом, складывающиеся в процессе жизнедеятельности по поводу оборота информации, доступ к которой ограничен. [20]

Т. А. Полякова и А. А. Стрельцов считают более корректным использовать понятие «режим тайн». [21]

Общественные отношения, складывающиеся по поводу тайны, принято называть конфиденциальными отношениями. Вообще слово «конфиденциальный» имеет латинское происхождение и употребляется в двух значениях: первое – доверительный, второе – секретный. [22] Поэтому все тайноотношения (общественные отношения, возникающие по поводу хранения, использования, передачи сведений, отнесенных к тому или иному виду тайн) по своей природе являются отношениями, основанными на доверии. На наличие «доверительного, то есть тайного способа информационного обеспечения системы принятия решений» указывает в своих научных работах и П. У. Кузнецов. [23]

Детально природа и структура доверительных отношений была исследована А. Н. Кокотовым. В таких отношениях существуют стороны, предмет и содержание. [24] В качестве сторон доверительных отношений А. Н. Кокотов выделяет доверяющего – лицо, которое доверяет (или доверилось), которое явилось инициатором, организатором доверия-отношения, и сторону, которой доверяют (которой доверились). [25] Под предметом доверительных отношений им понимается то, что доверяют. [26] Предметом тайноотношений как вида доверительных отношений могут являться определенные сведения ограниченного доступа. Соответственно, идеальным содержанием таких отношений будет сохранение доверенных сведений в тайне.

Учитывая лингвистические и теоретические признаки тайны, можно сделать вывод о ее информационной сущности.

1. Тайна – скрытая от восприятия существующая действительность (объективная реальность).

2. Тайна – искусственно созданная «маскировка» существующей действительности, приведение ее в состояние неопределенности (энтропии).

3. Тайноотношения – специфическая информационная деятельность, связанная с доверием и секретами, направленная на введение в конфиденциальное состояние информации, т.е. приведение ее в неузнаваемый вид.

По мнению П. У. Кузнецова сущность понятия «тайна» определяется его тремя его существенными признаками: [27]

1. Конфиденциальность сведений об особенностях жизни, которые подлежат сохранности от третьих лиц.

2.Особая важность событий, объектов и отдельных направлений человеческой деятельности.

3. Обязательность правовой защиты сохранности конфиденциальности сведений о наиболее важных сторонах человеческой деятельности личности, общества и государства.

На основе названных признаков П. У. Кузнецов определяет охраняемую законом тайну как установленное законом состояние конфиденциальности информации об особо важных сторонах жизни и деятельности личности, общества и государства. [28]

Представляется, что указанное определение тайны гармонизирует названные правовые позиции Л. Е. Владимирова, Л. О. Красавчиковой, А. А. Фатьянова, О. А. Городова, М. В. Пермякова, Э. Ф. Шамсумовой.

Несмотря на обозначенные выше общие особенности природы и характера складывающихся общественных отношений, каждый вид тайн обладает своей уникальной спецификой, что дополнительно указывает на тайну как на правовую категорию.

Стоит заметить, что в логическом аппарате любой науки главную теоретическую нагрузку несут ее основные, фундаментальные понятия – категории. [29]

Правовые категории – это предельные по уровню обобщения фундаментальные абстрактные понятия теории правоведения. [30]

Тайна является в силу своей уникальной природы общеправовой категорией, используемой всеми отраслями права, что находит свое отражение в десятках законодательных актах, в свою очередь вводящих в правовой оборот различные виды информации, охраняемые в режиме тайны.

Стоит заметить, что категории, будучи отражением, наиболее существенных свойств, главных связей правовых явлений, представляют собой наиболее глубокие по содержа-

нию и широкие по объему понятия в границах правовой науки. [31] Названное определение тайны П. У. Кузнецова всецело отвечает указанным общетеоретическим признакам правовой категории.

На сегодняшний день, можно констатировать отсутствие терминологического единства, как и единообразного понимания законодателем сути правовой категории тайны: в одном случае тайна предстает как правовой режим, в прочих – как правовой институт, опирающийся на понятие сведений. [32]

По мнению И. Л. Бачило, следствием отсутствия единства в понимании феномена тайны стала недостаточная проработанность, тяжеловесность и трудность для восприятия текстов многих правовых актов в области правового регулирования конфиденциальных отношений. [33] Право, использующее некорректные определения не будет исполнимым, непоследовательность законодателя в вопросе правового определения тайны уже сегодня ведет к ошибкам практике правового регулирования.

Примечания

1. Фатьянов А. А. Тайна и право (основные системы ограничения на доступ к информации в российском праве). М., 1999. С. 6.

2. Черных Г. Я. Историко-этимологический словарь современного рус¬ского языка, М.1993. Т.2 С.224. Цит. по Фатьянову А. А. Тайна и право (основные системы ограничения на доступ к информации в российском праве). М., 1999. С. 6

3. Даль В. И. Толковый словарь живого великорусского языка: в 4 т. Т.4., М.2002. С. 368; Старославянский словарь (по рукописям X-XI веков): около 10 000 слов: 2-е изд. / Сост. Э. Благова, Р. М. Цейтлин, С. Геродес, и др. Под. ред. Р. М. Цейтлин, Р. Вечерки и Э. Благовой: М., 1994. С.686-687.

4. Даль В. И. Указ. Соч. С. 368.

5. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка, М. 1997. С. 787.

6. Ушаков Д. Н. Толковый словарь русского языка. В 4 т. Т.4. М., 2000. С.316

7. Ефремова Т. Ф. Современный толковый словарь русского языка. В 3 т. Т.3. Р – Я. М., 2006. С.236

8. Ефремова Т. Ф. Указ. соч. С.236

9. Ефремова Т. Ф. Указ. соч. С.237

10. Ефремова Т. Ф. Указ. соч. С.237

11. Фатьянов А. А. Правовое обеспечение безопасности информации в Российской Федерации. М., 2001. С.46.

12. Там же.

13. Розенберг В. В. Промысловая тайна. СПб., 1910. С.1

14. Кузнецов П. У. Теоретические основания информационного права / Дис… док. юрид. наук. Екатеринбург, 2006. С. 190-191.

15. Кузнецов П. У. Теоретические основания информационного права / Дис… док. юрид. наук. Екатеринбург, 2006. С. 190-191.

16. Информационное право. Актуальные проблемы теории и практики. Под редакцией И. Л. Бачило. М.: Юрайт, 2009. С. 453.

17. Владимиров Л.Е. Учение об уголовных доказательствах. СПб., 1910. С.302

18. Красавчикова Л. О. Личная жизнь под охраной закона. М., 1983. С. 119.

19. Городов О. А. Информационное права: учебник для бакалавров. Москва: Проспект, 2013. С.63-64.

20. Пермяков М. В., Шамсумова Э. Ф. «Тайна» в праве. Екатеринбург : УралЮрИздат, 2006. С.46.

21. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2016. С.160

22. Confidentia буквально переводится с латинского как доверие. Советский энциклопедический словарь. М., 1985. С.623.

23. П. У. Кузнецов Теория и практика формирования правового режима коммерческой тайны. Сборник материалов летней сессии «ИНФОФОРУМА-5» - 5-й Всероссийской конференции «Информационная безопасность России в условиях глобального информационного общества» / Под. ред. А. В. Жукова. М., 2003. С. 39.

24. Кокотов А. Н. Доверие. Недоверие. Право. М., 2004. С. 16.

25. См.: Кокотов А. Н. Указ. соч. С.16-17.

26. См.: Кокотов А. Н. Указ. соч. С. 18.

27. Кузнецов П. У. Основы информационного права: учебник для бакалавров. М.: Проспект, 2014. С.208-209

28. Кузнецов П. У. Указ. соч. С.210

29. Васильев А. М. Правовые категории. М. Юридическая литература, 1976. С.57

30. См.: Васильев А. М. Указ. соч. С. 58.

31. См.: Васильев А. М. Указ. соч. С. 58.

32. Балашкина И.В. Тайна как разновидность информации: философско-правовые основания // Информационное право. 2010. N 1. С. 3

33. Информационное право. Актуальные проблемы теории и практики. Под редакцией И. Л. Бачило. М.: Юрайт, 2009. С. 453-545.

Паршуков Михаил Игоревич, доцент кафедры информационного права ФГБОУ ВПО Уральского государственного юридического университета, кандидат юридических наук, доцент. 620000, г.Екатеринбург, ул.Комсомольская, 23, каб.206. E-mail: m-parshukov@mail.ru

Parshukov Mikhail, Associate Professor of Information Law Ural State Law University , PhD, Associate Professor. 620000, Ekaterinburg, Komsomolskaya, 23-206. E-mail: m-parshukov@mail.ru

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ

Объем статьи не должен превышать 40 тыс. знаков, включая пробелы, и не может быть меньше 5 страниц. Статья набирается в текстовом редакторе Microsoft Word в формате *.rtf шрифтом Times New Roman, размером 14 пунктов, в полуторном интервале. Отступ красной строки: в тексте — 10 мм, в затекстовых примечаниях (концевых сносках) отступы и выступы строк не ставятся. Точное количество знаков можно определить через меню текстового редактора Microsoft Word (Сервис — Статистика — Учитывать все сноски).

Параметры документа: верхнее и нижнее поле — 20 мм, правое — 15 мм, левое — 30 мм.

В начале статьи помещаются: инициалы и фамилия автора (авторов), название статьи, **аннотация** на русском языке объемом **не менее 700 знаков или 10 строк,** ниже отдельной строкой — ключевые слова. **Ключевые слова** приводятся в именительном падеже в количестве до десяти слов. Инициалы и фамилия автора (авторов) дублируются транслитерацией. **Должны быть переведены на английский язык название статьи, аннотация, ключевые слова.**

УДК
ББК

ОБРАЗЕЦ

А. А. Первый, Б. Б. Второй, В. В. Третий

НАЗВАНИЕ СТАТЬИ, ОТРАЖАЮЩЕЕ ЕЕ НАУЧНОЕ СОДЕРЖАНИЕ, ДЛИНОЙ НЕ БОЛЕЕ 12—15 СЛОВ

Аннотация набирается одним абзацем, отражает научное содержание статьи, содержит сведения о решаемой задаче, методах решения, результатах и выводах. Аннотация не содержит ссылок на рисунки, формулы, литературу и источники финансирования. Рекомендуемый объем аннотации — около 50 слов, максимальный — не более 500 знаков (включая пробелы).

Ключевые слова: список из нескольких ключевых слов или словосочетаний, которые характеризуют Вашу работу.

Рисунки

Вставляются в документ целиком (не ссылки). Рекомендуются черно-белые рисунки с разрешением от 300 до 600 dpi. Подрисуночная подпись формируется как надпись («Вставка», затем «Надпись», без линий и заливки). Надпись и рисунок затем группируются, и устанавливается режим обтекания объекта «вокруг рамки». Размер надписей на рисунках и размер подрисуночных подписей должен соответствовать шрифту Times New Roman, 8 pt, полужирный. Точка в конце подрисуночной подписи не ставится. На все рисунки в тексте должны быть ссылки.

Все разделительные линии, указатели, оси и линии на графиках и рисунках должны иметь толщину не менее 0,5 pt и черный цвет. Эти рекомендации касаются всех графических объектов и объясняются ограниченной разрешающей способностью печатного оборудования.

Формулы

Набираются со следующими установками: стиль математический (цифры, функции и текст — прямой шрифт, переменные — курсив), основной шрифт — Times New Roman 11 pt, показатели степени 71 % и 58 %. Выключенные формулы должны быть выровнены по центру. Формулы, на которые есть ссылка в тексте, необходимо пронумеровать (сплошная нумерация). Расшифровка обозначений, принятых в формуле, производится в порядке их использования в формуле. Использование букв кириллицы в формулах не рекомендуется.

Таблицы

Создавайте таблицы, используя возможности редактора MS Word или Excel. Над таблицей пишется слово «Таблица», Times New Roman, 10 pt, полужирный, затем пробел и ее номер, выравнивание по правому краю таблицы. Далее без абзацного отступа следует таблица. На все таблицы в тексте должны быть ссылки (например, табл. 1).

Примечания

Источники располагаются в порядке цитирования и оформляются по ГОСТ 7.05-2008.

Статья публикуется впервые
Подпись, дата

В конце статьи перед данными об авторе должна быть надпись *«Статья публикуется впервые»,* ставится дата и авторучкой подпись автора (авторов). При пересылке статьи электронной почтой подпись автора сканируется в черно-белом режиме, сохраняется в формате *.tif или *.jpg и вставляется в документ ниже затекстовых сносок. (Либо сканируется последняя страница статьи с подписью и высылается по электронной почте отдельным файлом.)

Обязательно для заполнения: в конце статьи (в одном файле) на русском языке помещаются сведения об авторе (авторах) — полностью имя, отчество, фамилия, затем ученая степень, ученое звание, должность, кафедра, вуз (или организация, в которой работает автор); рабочий адрес вуза или организации (полные – включая название, город и страну – адресные сведения вместе с почтовым индексом, указывать правильное полное название организации, желательно – его официально принятый английский вариант), электронный адрес и контактные телефоны. **Эти данные об авторе должны быть переведены на английский язык.**

Для рассмотрения вопроса о публикации статьи в редакцию журнала необходимо выслать на электронную почту:

1) рукопись статьи, подписанную на последней странице всеми авторами. В рукописи должны быть полные сведения об авторах;

2) в случае, если статья имеет рецензию и заверена печатью, ее оригинал необходимо отправить в редакцию и по электронной почте в отсканированном виде с обязательным указанием контактов рецензента;

3) на статью необходимо выслать экспертное заключение о возможности открытого опубликования (образцы: заключение от руководителя эксперта (см. стр. 58) или заключение от экспертной комиссии (см. стр. 59)).

Библиографические ссылки

Цитируемая в статье литература приводится в виде списка в конце текста. В тексте в квадратных скобках дается ссылка на порядковый номер списка (ГОСТ Р 7.0.5.-2008). Полный текст ГОСТа размещен на официальном сайте Федерального агентства по техническому регулированию и метрологии Авторские примечания (не являющиеся используемой литературой или ссылкой на источник) размещаются в постраничных сносках.

Ниже приводятся образцы оформления сносок:

а) на монографии:

[1] Белова М. С., Кинсбурская В. А., Ялбулганова А. А. Налоговый контроль и ответственность: анализ законодательства, административной и судебной практики / под ред. А. А. Ялбулганова.— М. : Знание, 2008.— С. 12.

б) на статьи из сборников:

[1] Клишина М. А. Новое в порядке составления проекта бюджета // Финансовое право России: актуальные проблемы / под ред. А. А. Ялбулганова.— М., 2007.— С. 101.

в) статьи из журналов и продолжающихся изданий:

[1] Глушко Е. К. Административно-правовая природа государственных корпораций // Реформы и право.— 2008.— № 3.— С. 38—43.

г) авторефераты диссертаций:

[1] Стрижова О. А. Правовое регулирование таможенной стоимости : автореф. дис. … канд. юрид. наук.— М., 2008.— С. 7.

д) интернет-страницы:

Противодействие коррупционным правонарушениям // Юридическая Россия: федеральный правовой портал. URL: http://law.edu.ru/news/news.asp?newsID=12954 (дата обращения: 08.01.2009).

В редакцию журнала статья передается качественно по электронной почте одним файлом (название файла — фамилия автора). Тема электронного письма: Вестник УрФО. Безопасность в информационной сфере.

Отправляемая статья должна быть вычитана автором; устранены все грамматические, пунктуационные, синтаксические ошибки, неточности; выверены все юридические и научные термины. За ошибки и неточности научного и фактического характера ответственность несет автор (авторы) статьи.

Поступившие в редакцию материалы возврату не подлежат.

Материалы к публикации отправлять по адресу E-mail: urvest@mail.ru в редакцию журнала «Вестник УрФО. Безопасность в информационной сфере».

Или по почте по адресу: Россия, 454080, г. Челябинск, пр. им. Ленина, д. 76, ЮУрГУ, Издательский центр.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ

УТВЕРЖДАЮ
Должность руководителя
организации или лица с
соответствующими полномочиями
_____И. О. Фамилия
«___»_____2015 г.

ЗАКЛЮЧЕНИЕ № _____

о возможности открытого опубликования

_____
(наименование материалов, подлежащих экспертизе)

Руководитель-эксперт[1] _____

в период с «___»_____20___г. по «___»_____20___г. провел экспертизу материалов

_____
(наименование материалов, подлежащих экспертизе)

на предмет отсутствия (наличия) в них сведений, составляющих государственную тайну, и сведений, подпадающих под действие законодательства об экспортном контроле, и возможности (невозможности) их открытого опубликования.

Руководствуясь Законом Российской Федерации «О государственной тайне», Перечнем сведений, отнесенных к государственной тайне, утвержденным Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203, а также Перечнем сведений, подлежащих засекречиванию Министерства образования и науки РФ, утвержденным приказом Минобрнауки РФ № 36с от 10.11.2014 г., а также Федеральным законом «Об экспертном контроле» от 18.07.1999 г. № 183-ФЗ и Указами Президента РФ № 1661 от 17.12.2011 г., № 1005 от 08.08.2001 г., № 36 от 14.01.2003 г., № 202 от 14.02.1996 г., № 1083 от 20.08.2007 г., № 1082 от 28.08.2001 г., руководитель-эксперт установил:

1) Сведения, содержащиеся в рассматриваемых материалах, находятся в компетенции *Наименование организации.*

2) Сведения, содержащиеся в рассматриваемых материалах, _____

_____
(указываются сведения, содержащиеся в материалах)

не подпадают под действие Перечня сведений, составляющих государственную тайну (статья 5 Закона Российской Федерации «О государственной тайне»), не относятся к Перечню сведений, отнесенных к государственной тайне, утвержденному Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203, не подлежат засекречиванию, не подпадают под действие законодательства об экспортном контроле и данные материалы могут быть открыто опубликованы.

Руководитель-эксперт (Ф.И.О., подпись)

Секретарь ЭК (Ф.И.О., подпись)

[1] Если экспертиза материалов проводится руководителем структурного подразделения университета, в котором работает автор подготовленных материалов

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ

УТВЕРЖДАЮ
Должность руководителя
организации или лица с
соответствующими полномочиями
_____И. О. Фамилия
«___»_____2015 г.

ЗАКЛЮЧЕНИЕ № _____

о возможности открытого опубликования

_____
(наименование материалов, подлежащих экспертизе)

Экспертная комиссия в составе _____

в период с «___»_____20___г. по «___»_____20___г. провела экспертизу материалов

_____
(наименование материалов, подлежащих экспертизе)

на предмет отсутствия (наличия) в них сведений, составляющих государственную тайну, и сведений, подпадающих под действие законодательства об экспортном контроле, и возможности (невозможности) их открытого опубликования.

Руководствуясь Законом Российской Федерации «О государственной тайне», Перечнем сведений, отнесенных к государственной тайне, утвержденным Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203, а также Перечнем сведений, подлежащих засекречиванию Министерства образования и науки РФ, утвержденным приказом Минобрнауки РФ № 36с от 10.11.2014 г., а также Федеральным законом «Об экспертном контроле» от 18.07.1999 г. № 183-ФЗ и Указами Президента РФ № 1661 от 17.12.2011г, № 1005 от 08.08.2001 г., № 36 от 14.01.2003 г., № 202 от 14.02.1996 г., № 1083 от 20.08.2007 г., № 1082 от 28.08.2001 г., экспертная комиссия установила:

1) Сведения, содержащиеся в рассматриваемых материалах, находятся в компетенции *Наименование организации.*

2) Сведения, содержащиеся в рассматриваемых материалах, _____

_____
(указываются сведения, содержащиеся в материалах)

не подпадают под действие Перечня сведений, составляющих государственную тайну (статья 5 Закона Российской Федерации «О государственной тайне»), не относятся к Перечню сведений, отнесенных к государственной тайне, утвержденному Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203, не подлежат засекречиванию, не подпадают под действие законодательства об экспортном контроле и данные материалы могут быть открыто опубликованы.

Председатель комиссии (Ф.И.О., подпись)

Члены ЭК : (Ф.И.О., подпись)

Секретарь ЭК (Ф.И.О., подпись)

ВЕСТНИК УрФО
Безопасность в информационной сфере № 4(22) / 2016

Дата выхода в свет 30.12.2016. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 7,0. Тираж 100 экз. Заказ 470/486.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 4(22) / 2016

Date of publication of the 30.12.2016. Format 70×108 1/16. Screen printing.
Conventional printed sheet 7,0. Circulation – 100 issues. Order 470/486. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080