3. Показано, что предложенный метод контроля показателя pH применим для автоматизации технологических процессов нейтрализации загрязненных мелкодисперсными включениями кислот и щелочей в условиях промышленных предприятий.

ЛИТЕРАТУРА

1. **Брусиловский Л. П., Вайнберг А. Я.** Приборы технологического контроля в молочной промышленности: Справ. – 2-е изд., перераб. и доп. – М.: Агропромиздат, 1990. – 288 с.

2. **Кантере В. М., Казаков А. В., Кулаков М. В.** Потенциометрические и титрометрические приборы. – М.: Машиностроение, 1970. – 304 с.

3. **Киреев В. А.** Краткий курс физической химии. – М.: Химия, 1969. – 639 с.

4. **Определение** типа и концентрации растворов электролитов на основе анализа потенциодинамических кривых / Р. И. Воробей, О. К. Гусев, В. П. Киреенко и др. // Вестник БНТУ. – 2003. – № 2. – С. 48–53.

УДК 681.324.067

КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПО ПРИЗНАКУ ОТКРЫТОСТИ В РАМКАХ СУЩЕСТВУЮЩИХ ПРАВОВЫХ ДОКУМЕНТОВ РЕСПУБЛИКИ БЕЛАРУСЬ

Канд. техн. наук КРОТЮК Ю. М., асп. ТРЕТЬЯКОВИЧ К. В., юрист МАКУТИНА И. В.

НП РУП «Научно-исследовательский институт технической защиты информации», Белорусский национальный технический университет

Анализ классификационных аспектов описания информационных ресурсов по критериям информационной безопасности нашел отражение в [1...3]. Предлагались возможные классификации информационных ресурсов, в основе которых рассматривались существенные, с точки зрения обеспечения безопасности, признаки информации: содержание, источники, форма собственности на информационный ресурс, назначение, степень открытости и объем информационных ресурсов. В основе классификации информационных ресурсов по критерию открытости, исходя из анализа правовых документов Республики Беларусь, лежит признак содержания информационных ресурсов. В [2] описаны пять способов классификации информации с точки зрения ее содержания, обозначенные как тематический, объектный, предметный, локальный и традиционный.

На основе проведенного в [2] анализа делается вывод о том, что задаче классификации информационных ресурсов по критериям информационной безопасности в наибольшей степени соответствуют тематический и объектный способы описания. При этом их практическое применение также связано с рядом трудностей и противоречий [1].

Настоящая работа посвящена анализу классификационных аспектов описания информационных ресурсов по критерию открытости в рамках существующих правовых документов Республики Беларусь. При этом открытость рассматривается как инверсное отображение конфиденциальности.

Термины и определения, согласно [4]:

- информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах;
- документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- информационный ресурс – организованная совокупность документированной информации, включающая базы данных и знаний, другие массивы информации в информационных системах;

• собственник информационных ресурсов, информационных систем, технологий, средств их обеспечения – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения данными объектами.

Принятый в 2001 г. в качестве предстандарта Республики Беларусь СТБ 34.101.1–2001 «Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий», часть 1, соответствующий международному стандарту ИСО/МЭК 15408–1:1999 «Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Введение и общая модель», часть 1, рассматривает следующие виды защиты информации и соответствующие им категории защиты информации:

• защита от несанкционированного раскрытия – категория «конфиденциальность»;

• защита от несанкционированного изменения – категория «целостность»;

• защита от невозможности использования – категория «доступность».

Эти категории являются сущностью проблемы информационной безопасности, с точки зрения которых возможны различные способы классификации информационных ресурсов по признаку существенности для информационной безопасности.

Категории «целостность» и «доступность» направлены на защиту неотъемлемых свойств информационных ресурсов и возможностей использования этих свойств собственником информационных ресурсов. Категория «конфиденциальность» направлена на обеспечение вводимого собственником информационного ресурса ограничений на возможность несанкционированного доступа к этой информации. При этом свойства самой информации определяют процедуру ее отнесения к категории конфиденциальной и в дальнейшем не учитываются. Таким образом, «конфиденциальность» является обособленной категорией защиты информационных ресурсов, ее анализ необходимо проводить при проектировании любых информационных систем независимо от их прикладного назначения в связи с необходимостью приведения в соответствие с действующим законодательством принимаемых мер защиты.

Согласно [4], вопрос о конфиденциальности или степени закрытости информационных ресурсов, как правило, решает владелец этого ресурса. Исключение составляют случаи, связанные с государственными секретами, при которых решения о степени закрытости информационных ресурсов принимает наделенный соответствующими полномочиями орган государственного управления, а также случаи, связанные со сведениями, доступ к которым запрещено ограничивать действующими правовыми документами.

Использование в целях классификации информационных ресурсов категории конфиденциальности информации предполагает рассмотрение в рамках этой классификации только тех информационных ресурсов, доступ к которым в той или иной степени ограничен. В этой связи более общим случаем является использование в целях классификации информационных ресурсов признака открытости информации, который подразумевает классификацию всего спектра информационных ресурсов, так как не существует информационных ресурсов, которые являются закрытыми для всех.

Несмотря на то, что, казалось бы, существует достаточно простая и общепринятая классификация категорий открытости информации, которая может быть положена в основу классификации информационных ресурсов по критерию открытости [4...7], например секретная информация, информация ограниченного распространения, информация, составляющая служебную или коммерческую тайну, при разработке правовых и нормативных документов, регулирующих вопросы защиты информации, возникла терминологическая неясность в использовании понятий «защита информации» и «ограничение доступа к информации».

В законодательных актах, так или иначе регулирующих вопросы доступа к информации и информационным ресурсам [8], содержатся сведения о том, что право на защиту от незаконного использования информации возникает лишь в том случае, если информация отнесена к категориям «служебная тайна» или «коммерческая тайна». Иными словами, нельзя осуществлять защиту информации, не закрываемой по закону. Аналогичные выводы в явном или косвенном виде имеются и в работах авторов

[2], проводивших анализ вопросов защиты информационных ресурсов. При этом не принимается во внимание тот факт, что ограничение доступа к информации в процессе технологического цикла и обработки является неотъемлемым условием обеспечения работоспособности организации в целом и информационной системы организации в частности.

В соответствии с [4] защита документированной информации, не имеющей государственного значения, устанавливается в порядке, предусмотренном ее собственником либо собственником информационной системы либо уполномоченными государственными органами. Таким образом, собственник вправе вводить ограничения на доступ к своим информационным ресурсам в процессе их накопления, обработки и хранения, установив порядок доступа к этим ресурсам, если право доступа к ним закреплено законодательно.

Проблема классификации информационных ресурсов по признаку открытости распадается на две части [1]: точность классификации и правомерность отнесения информационных ресурсов к той или иной категории открытости.

Первая часть проблемы заключается в том, что различные категории открытости информационных ресурсов определены в действующем законодательстве с разной степенью детализации. Достаточно детально определены категории, связанные с секретной информацией (сведения, отнесенные к государственной тайне) [2]. Менее точно отражены сведения, содержащие информацию ограниченного распространения в соответствии с республиканским перечнем сведений ограниченного распространения.

Вопросы, касающиеся «коммерческой тайны» и «служебной тайны», отражены в законодательстве поверхностно. Кроме того, категории «служебная тайна» в разных правовых документах придается разное значение. Так, в [5] – это категория государственных секретов, разглашение или утрата которых могут причинить существенный вред национальной безопасности, а в [8] – это сведения, разглашение которых способно нанести ущерб деятельности собственника. Достаточно неопределенной является и категория «профессиональная тайна».

Тем не менее, любые работы по защите информационных ресурсов нуждаются в классификации информации по признаку открытости, и в этой связи обобщенная классификация информации по указанному признаку, ориентированная на систему действующих в Беларуси нормативных документов, представляет интерес. Указанная классификация представлена на рис. 1. Целями защиты является сохранение конфиденциальности, полноты, точности, целостности документированной информации, возможности управления процессом обработки и использования в соответствии с условиями, установленными собственником этой информации или уполномоченным лицом [4].

Если рассмотреть предложенную классификацию с позиций значимости информации для государства, то очевидно, что степень участия уполномоченных государственных органов в процедуре принятия решения об открытости тех или иных сведений убывает слева направо, а степень открытости информации соответственно возрастает. Однако, если в качестве количественного критерия оценки степени открытости тех или иных сведений выбрать численность осведомленных субъектов, то, вероятнее всего, наименее открытыми будут сведения из категории «коммерческая тайна». Это объясняется тем, что на практике носителями сведений об особенностях технологии ведения бизнеса, стратегии развития конкретного предприятия являются единичные субъекты, в то время как численность носителей государственных секретов в соответствии с [5] потенциально намного выше.

Вторая часть проблемы связана с правомерностью отнесения информационных ресурсов к той или иной категории открытости. В соответствии с законодательством присвоение категории открытости конкретным информационным ресурсам осуществляет их владелец в пределах своих полномочий в соответствии с [4, 5]. Учитывая невозможность детального определения сведений, доступ к которым ограничивается законодательством на всем информационном поле, а также имеющимися противоречивостью и неполнотой законодательства, очевидно, что возможны ошибки и злоупотребления или неумышленные нарушения законодательства.

Рис. 1

В предложенной классификации вводятся три класса информационных ресурсов: содержащие различные виды тайн, сведения из «Республиканского перечня сведений ограниченного распространения» и свободно распространяемые сведения. Первый класс объединяет государственные секреты и другие виды тайн. К государственным секретам в соответствии с [5] отнесены сведения, защищаемые государством в целях предотвращения их несанкционированного распространения и создания угрозы национальной безопасности страны, а также конституционным правам и свободам граждан. К служебной информации ограниченного распространения в соответствии с [6] отнесены сведения, распространение которых в соответствии с действующим законодательством Республики Беларусь организации считают нежелательным в интересах обеспечения своей деятельности.

Процедуры отнесения сведений к категории «государственные секреты» определены в [5]. Процедуры отнесения сведений к категории «служебная информация ограниченного распространения» в соответствии с правовыми документами определены в [6] и детализированы в других законодательных и нормативных актах.

В меньшей степени поддается формализации процедура отнесения информации к категориям «Служебная и коммерческая тайна», определенным в статье 140 Гражданского кодекса Республики Беларусь [8]. Вопросы, касающиеся принятия решения о степени открытости информации обладателем информационного ресурса, связаны с необходимостью анализа коммерческой ценности информационного ресурса и сопоставления этой ценности с затратами на реализацию механизмов ограничения доступа к этим информационным ресурсам. Сложность принятия решения обусловлена также тем, что действие указанной выше статьи распространяется на охрану государственных секретов. Таким образом, «служебная тайна», согласно [5, 8], относится к категории государственных секретов, однако тяжесть последствий разглашения сведений, отнесенных к этой категории, определена в законодательных актах по-разному.

Класс информационных ресурсов, содержащих свободно распространяемые сведения, включает сведения, ограничение распространения которых запрещено законодательно, а также сведения, которые не относятся ни к одному из видов тайн и не являются сведениями ограниченного распространения.

Предлагаемая в данной работе классификация информационных ресурсов по степени открытости информации не исключает возможности категорирования информационных ресурсов по критериям целостности и доступности или другим, тем не менее может быть использована при проектировании систем защиты информации для конкретных информационных систем.

Исходя из представленной классификации, которая соответствует структуре правовых документов Республики Беларусь, может быть определен порядок формирования и применения требований к уровню защищенности информационных ресурсов и программно-аппаратных средств, обеспечивающих реализацию информационных процессов. Информационные ресурсы, содержащие информацию государственного значения, в соответствии с представленной классификацией должны обрабатываться только в системах, обеспеченных защитой, необходимый уровень которой подтвержден сертификатом соответствия. К таким ресурсам относятся государственные секреты и служебная информация ограниченного распространения. Защита другой документированной информации устанавливается в порядке, предусмотренном ее собственником или собственником информационной системы [4].

ЛИТЕРАТУРА

1. **Антопольский А. Б.** Проблемы классификации информационных ресурсов // НТИ. Сер.7. – 1997. – № 8. – С. 1–12.

2. **Антопольский А. Б.** Проблемы классификации информационных ресурсов по критериям информационной безопасности // Информационные ресурсы России. – 1997. – № 6 (37).

3. **Коробкин А.** Информационные ресурсы: Проблемы классификации // Информационные ресурсы России. – 1997. – № 5 (36).

4. **Закон** Республики Беларусь «Об информатизации» // Ведомости Верховного Совета Республики Беларусь. – 1995. – № 33. – С. 428.

5. **Закон** Республики Беларусь «О государственных секретах» // Ведомости Верховного Совета Республики Беларусь. – 1995. – № 3. – С. 5.

6. **Постановление** Совета Министров Республики Беларусь № 237 от 15.02.1999 // Республиканский перечень сведений ограниченного распространения.

7. **Закон** Республики Беларусь «О печати и других средствах массовой информации» // Ведомости Верховного Совета Республики Беларусь. – 1995. – № 12. – С. 121.

8. **Гражданский** кодекс Республики Беларусь // Ведомости Верховного Совета Республики Беларусь. – 1999. – № 7–9. – С. 101.