Технологии и методики классификации информационных ресурсов

С. В. Симонов

Основные понятия и определения

Классификация информационных ресурсов — обязательный этап при проектировании подсистемы информационной безопасности. Требования к обеспечению режима информационной безопасности для различных классов ресурсов могут быть различными.

В методиках классификации, например [1, 4, 7], ключевым понятием является информационный ресурс.

Информационный ресурс — это определенный элемент информации, хранимый в любом виде (бумажном, электронном), который признается «ценным» для организации. Информация, которая включает в себя информационный ресурс, может представлять собой не только хорошо структурированную информацию, такую как списки клиентов или файл адресов. Она может представлять собой, к примеру, планы по выпуску нового продукта, маркетинговую информацию.

Независимо от характера самих информационных ресурсов, они обладают одной или несколькими из следующих характеристик:

- Они признаются ценными для организации.
- Их невозможно заменить без затрат средств, времени, иных ресурсов или их сочетания.
- Они существенно влияют на деятельность организации, без этих ресурсов возникает угроза для основной деятельности организации.

Классификация данных и документов производится, если необходимо разделить данные, которые обладают малой ценностью (если вообще обладают такой), и данные, которые весьма важны для организации.

При классификации данных предполагается, что:

- Все данные имеют владельца.
- Владелец данных или процесса должен классифицировать информацию, поместив ее в одну из категорий безопасности, в зависимости от юридических обязательств, затрат, корпоративной политики и коммерческих нужд.

- Владелец должен объявить, кто имеет доступ к данным.
- Владелец отвечает за такие данные и должен обеспечить, чтобы они были защищены (например, при помощи администратора безопасности) в соответствии с их классификацией.
- Все документ должны классифицироваться, и уровень классификации должен быть написан, по крайней мере, на заглавной странице.

Важность данных (информационного ресурса) — субъективное понятие, которое должно быть конкретизировано его владельцем. В общем случае, владелец информационного ресурса должен выбрать систему критериев, которые описывают разные аспекты конфиденциальности, целостности и доступности информации, а также ценность (стоимость) информационного ресурса.

На практике зачастую ограничиваются оценкой конфиденциальности данных и их ценности (стоимости).

Типовые системы классификации данных

Ниже приводятся типовые системы классификации данных по конфиденциальности и доступности в соответствии с [4, 7].

Конфиденциальность

Хранимые данные необходимо классифицировать с точки зрения уровня их конфиденциальности. Для многих организаций достаточно следующих 5 уровней (табл. 1).

Таблица 1

Классификация документа/данных	Описание
Строго конфиденциально	Весьма важные внутренние документы, например документы о предполагаемых слияниях или приобретениях; инвестиционные стратегии; планы и проекты; информация, которая может существенно повредить организации, если она будет утрачена или станет широкодоступной. Информация, классифицируемая как строго конфиденциальная, имеет очень ограниченный круг распространения и должна быть всегда защищена. Для этого уровня обеспечивается самый высокий уровень защиты.
Высоко конфиденциально	Информация, которая, если станет широкодоступной или даже широко известной внутри организации, может серьезно помешать осуществлению операций организации и считается очень важной для ее текущих операций. Такая информация может включать бухгалтерские данные, бизнес-планы, клиентские сведения о банках, адвокатах и бухгалтерах и т. п., медицинские сведения пациентов и аналогичные высоко конфиденциальные данные. Такая информация не должна копироваться или удаляться из сферы оперативного контроля организации без специального разрешения. Для этого уровня необходимо обеспечить адекватный высокий уровень защиты.

Окончание таблицы 1

Управленческая информация	Процедуры, оперативные устоявшиеся практики, планы проектов, дизайны и спецификации, которые определяют порядок, в соответствии с которым работает организация. Такая информация обычно предназначена для ограниченного использования исключительно уполномоченным персоналом. Для этого уровня обеспечивается адекватный высокий уровень защиты.
Для внутреннего использования	Информация, которую не предполагается широко распространять за пределами организации, и потеря которой может повлечь за собой различного рода неприятности для организации или руководства, но ее раскрытие вряд ли может привести к финансовому убытку или серьезному подрыву доверия. Примеры могут включать внутренние служебные записки, протоколы собраний, внутренние отчеты о проектах. В данном случае уровень защиты контролируется, но является обычным.
Открытая информация	Широкодоступная информация; годовые отчеты, заявления для прессы и т. п.; информация, которая предназначена для широкого использования. Конфиденциальность на этом уровне не обеспечивается.

Доступность

Рассмотрим пример классификации, имеющей четыре класса (1–4). Подобная классификация может применяться для корпоративной системы документооборота (табл. 2).

Таблица 2

Класс	1	2	3	4
Максимально допустимое время простоя сервера, из расчета на одно событие	1 неделя	1 день	1 час	1 час
По каким дням	Пн–Пт	Пн–Пт	Пн–Пт	7 дней
В какие часы?			07:00–18:00	24 ч
Оценка доступности (% времени)	80 %	95 %	99,5 %	99,9 %
Ожидаемое максимальное время простоя	= 1 день/неделя	= 2 часа/неделя	= 20 мин./неделя	= 12 мин./месяц

Для повышения доступности, профилактические меры снижают вероятность простоя, а восстановительные меры снижают время простоя после инцидента.

Стоимость информационных ресурсов

Для некоторых информационных ресурсов их владелец может определить (задать) стоимость. Подразумевается, что информация не является об-

щедоступной и приведет к убыткам, ущербу или даже к краху бизнеса, если она будет потеряна, украдена или скомпрометирована каким-либо образом.

Оценка стоимость (ценность) ресурсов позволяет выстроить систему приоритетов при защите активов, которые обладают повышенной ценностью.

Стоимость может быть выражена в денежных единицах или в качественных шкалах, например: незначительный ущерб, существенный ущерб, и т. д. При этом используемые качественные шкалы должны быть точно определены, как это было сделано в рассмотренных выше примерах.

Процедура классификации данных

Процедура классификации включает ряд этапов. Одна из рекомендаций («good practices») [4], обобщающих практику проведения таких работ, предлагает следующий список этапов:

1. Сформулировать ясные цели классификации. Цели должны быть сформулированы в письменном виде, доведены до всех причастных к процедуре лиц (владельцев информационных ресурсов) и быть ясны для них. Заявленные цели должны быть реалистичны, т. е. желательно использовать принцип разумной достаточности. Усилия и ресурсы, направленные на реализацию данного проекта, не должны быть чрезмерными.
2. Сформировать рабочую группу, включающую владельцев информационных ресурсов процессов и ресурсов, а также обслуживающий персонал, эксплуатирующий информационную систему. Задача этой рабочей группы — проведение классификации.
3. Провести ревизию существовавших в организации принципов классификации, сформулировать недостатки существующей системы. Эта работа может быть проведена в форме опроса членов рабочей группы. Результат работы — краткое изложение недостатков существовавшей системы классификации с позиции сегодняшнего дня и с учетом перспектив развития.
4. Изучить существующие системы классификации для аналогичных условий. Как показывает практика, в большинстве случаев за основу может быть взята подходящая система классификации, которую потребуется немного модернизировать.
5. Верифицировать выбранную процедуру классификации. Необходимо убедиться, что:
   - выбранное число классов оптимально, т. е. правильно выбран компромисс между сложностью системы классификации (числом клас-

сов) и ее функциональностью (простотой практического применения, соответствия поставленным целям);

- система классификации интуитивно понятна для всех участников проекта. Описания классов должны быть четкими, исключающими неоднозначное толкование.

6. Оценить совместимость системы классификации с существующими формальными правилами и процедурами. Возможно, потребуется внесение изменений в утыерженные формальные правила и процедуры.
7. Оценить воздействие вновь принимаемой системы классификации на технологию обработки данных. Такое воздействие в ряде случаев может быть существенным и потребовать внесения изменений в существующую технологию обработки информации.
8. Установить процедуру периодического пересмотра системы классификации. Любая система классификации должна периодически пересматриваться, при необходимости в нее должны вноситься изменения. Период времени, через который эта процедура повторяется зависит от специфики информационного процесса.
9. Необходимо наметить дальнейшие шаги по совершенствованию системы управления для данной информационной технологии. Разработка системы классификации не может быть самоцелью, не связанной с другими, более общими целями.

Примеры методик классификации данных

Классификация данных, принятая в университете штата Массачусетс

В данном примере в основу классификации положены: конфиденциальность и ценность информационного ресурса.

Классификация университетских данных [6] основана на следующих законах: Закон о вторжении в частную жизнь и правах на образование 1974 г. (с изменениями) 20 U.S.C. 1232g и нормами, провозглашенными на их основе, 34 C.F.R., Часть 99; Закон Массачусетса о справедливых информационных практиках, M.G.L. c66A, и Закон Массачусетса об общедоступных данных, M.G.L. c. 66, раздел 10.

Данные классифицируются по следующим категориям:

- Несекретные — данные, которые не подпадают в любые другие классификационные категории, отмеченные ниже. Эти данные могут быть широко доступны без специального одобрения хранителя данных.

- Только для оперативного использования — данные, потеря, порча или несанкционированное разглашение которых может привести к любому коммерческому, финансовому или юридическому убытку, и которые предоставляются исключительно пользователям, одобренным хранителем данных.
- Частные — данные, разглашение которых может привести к любому коммерческому, финансовому или юридическому убытку, и которые связаны с вопросами личного доверия, репутации или другими вопросами неприкосновенности личной жизни.
- Ограниченного пользования — данные, потеря, порча или несанкционированное разглашение которых может привести к нанесению ущерба коммерческим или исследовательским функциям Университета или к коммерческому, финансовому или юридическому убытку.
- Конфиденциальные — данные, потеря, порча или несанкционированное разглашение которых может привести к нарушению федеральных законов/положений, законов/положений штата или университетских контрактов.

Университетские процедуры, касающиеся защиты и классификации данных, предусматривают следующее:

- Совокупности данных должны классифицироваться на уровне самого высокого уровня защиты (например, если в одной и той же базе данных, файле, отчете и т. п. имеются данные, относящиеся к различным классификационным категориям, классификационная категория такой базы данных, файла или отчета соответствует их категории самого высокого уровня).
- Базы данных, содержащие «Только для оперативного использования», «Частные», «Ограниченного пользования» или «Конфиденциальные» данные, должны быть защищены. Извлечения из файлов данных «Только для оперативного использования», «Частных», «Ограниченного пользования» или «Конфиденциальных» данных должны быть защищены на том же уровне, что и файл/база данных, из которых такие данные извлекаются.

Отчеты, содержащие «Только для оперативного использования», «Частные», «Ограниченного пользования» или «Конфиденциальные» данные, должны надлежащим образом утилизироваться.

Если система содержит данные, входящие в несколько классов, они должны быть отнесены к самым конфиденциальным данным в системе.

Информация, относящаяся к государственной тайне в США. Классификация и критерии оценки

В 80-х гг. в США был принят следующий список областей, относящихся к национальной безопасности США [2, 3]:

- Военные планы, вооружения.
- Характеристики систем вооружения и их слабости.
- Закрытые данные об иностранных государствах.
- Деятельность спецслужб, методы спецслужб.
- Международные отношения и связанные с ней действия правительственных структур США.
- Научно-технические материалы, имеющие отношение к национальной безопасности.
- Программы правительства по обеспечению сохранности ядерных материалов.
- Криптография.
- Прочие области, относящиеся к национальной безопасности.

При принятии решения относительно ограничения доступа к информации определенной категории, принимаются во внимание как потенциальные **риски**, связанные с раскрытием информации), так и **стоимость классификации** (совокупность факторов, препятствующих закрытию информации).

При оценке **рисков**, связанных с раскрытием конфиденциальных данных, принимаются во внимание следующие факторы:

- Помощь другим станам в создании новых систем вооружения.
- Помощь другим станам в совершенствовании существующих систем вооружения.
- Помощь другим станам в создании материалов для новых систем оружия.
- Ущерб в области международных отношений, переговорах о сокращении вооружений, блокировании внешних угроз
- Любые другие виды ущерба в области национальной безопасности США в перечисленных выше областях.

Стоимость классификации

Учитывается ряд **факторов**, препятствующих закрытию информации:

- Данная информация, остающаяся в открытом (общедоступном) виде, содействует прогрессу в разных областях в США.

- Затраты, связанные с классификацией и мероприятиями по закрытию информации.
- Прямая экономическая выгода от использования данных (информации) в промышленности США.
- Выгоды в связи с доступностью информации в области международных отношений, контролем над вооружениями, торговле.
- Повышение доверия к программам по классификации.
- Данная информация, остающаяся в открытом (общедоступном) виде, содействует публичным дискуссиям и образованию.
- Данная информация, остающаяся в открытом (общедоступном) виде, способствует общемировому прогрессу в области науки и технологий.
- Данная информация, остающаяся в открытом (общедоступном) виде, способствует прогрессу национальной (США) науки и технологий.

Критерии, по которым оценивается ущерб от раскрытия данных, конкретизируют рассмотренные выше факторы.

В качестве примера рассматривается система критериев связанных с раскрытием неклассифицированной научной или технической информации [1].

Критерии оценки различных факторов (рисков и цены), связанных с раскрытием информации

Критерии, относящиеся к цене классификации

№	Описание критерия
1	Экономия, связанная с улучшением эффективности взаимодействия персонала
2	Экономия из-за устранения задержек, связанных с формальными процедурами доступа к информации
3	Экономия вследствие упрощения процедуры доступа к научно-технической информации для потребителей
4	Увеличение производительности труда как следствие внедрения в промышленность научно-технических данных
5	Улучшение способности ограничить доступ к закрытым данным за счет сокращения их объема
6	Уменьшение задержки доступа к данным за счет исключения процедур, связанных с классификацией данных

7 Уменьшение затрат на ПО, поскольку отпадает необходимость специальной разработки (заказное ПО) для разных типов данных

8 Уменьшение затрат на ПО, поскольку имеется возможность использовать однотипные процедуры

9 Уменьшение затрат на ПО, поскольку имеется возможность использовать стандартное ПО

10 Уменьшение стоимости подготовки документов

11 Уменьшение стоимости транспортировки

12 Уменьшение стоимости хранения

13 Исключение стоимости, вследствие исключения процедур пересмотра классификации

14 Исключение стоимости утилизации данных и носителей, имеющих гриф

15 Экономия на специализированных процедурах обеспечения безопасности

16 Экономия на расходах, связанных с объемом информации, защищаемой специализированными средствами и процедурами

17 Экономия на обеспечении персональной безопасности

18 Экономия рабочего времени персонала, не связанного в прямую с процедурами обеспечения безопасности закрытых данных

Критерии, относящиеся к общему прогрессу в области науки и технологии

19 Содействие прогрессу в области науки и технологии (прямой эффект)

20 Содействие прогрессу как следствие обмена идеями и информацией в данной сфере

Критерии, описывающие полезность информации для передачи технологий в коммерческий сектор

21 Содействие прогрессу отечественной (США) экономики в части создания новых продуктов и возможностей

22 Содействие прогрессу отечественной (США) экономики в части улучшения существующих продуктов

Критерии, относящиеся к международным отношениям

23 Содействие международным усилиям в области борьбы с терроризмом, распространением опасных видов оружия (ядерное, биологическое, …)

Критерии, относящиеся к образованию и развитию общества

24 Информация может быть использована для поддержки текущей политики

25 Информация полезна для освещения деятельности правительства

26 Информация может быть использована в для достижения приоритетных целей в деятельности правительственных структур

Критерии, относящиеся к другим приоритетным областям США

27 Информация может способствовать достижению целей США в прочих областях

Доверие к системе классификации

28 Информация может способствовать повышению доверия к системе классификации

Требования к режиму информационной безопасности

Введение классификации данных предполагает установление отдельных требований к режиму информационной безопасности для каждой категории. Пример таких требований приводится ниже.

Общедоступная / несекретная информация

Данные в таких системах должны быть общедоступными без последствий для компании (т. е. данные не являются конфиденциальными). Целостность данных не имеет значения. Выход из строя по причине злонамеренных атак является приемлемой опасностью.

Примеры: Тестовые сервисы без конфиденциальных данных, некоторые сервисы с общедоступной информацией, брошюры о продуктах широко распространены, и данные в любом случае доступны широкой общественности.

Внутренняя информация

Внешний доступ к этим данным должен быть запрещен, но если такие данные станут широко доступными, последствия не будут критическими (например, компания может оказаться в затруднительном положении в глазах общественности). Внутренний доступ — по выбору. Целостность данных важна, но не является жизненно важной.

Примеры данных этого типа можно найти в группах разработки (где нет реальных данных), некоторых производственных общественных службах, в том числе некоторые клиентские данные, «нормальные» рабочие документы и протоколы проектов/собраний, телефонные книги.

Конфиденциальная информация

Данные этого класса являются конфиденциальными внутри компании и защищены от внешнего доступа. Если к таким данным получили неуполномоченные лица, это может повлиять на текущую эффективность работы компании, причинить серьезный финансовый убыток, обеспечить значительную выгоду конкуренту или вызвать серьезное уменьшение доверия клиентов. Целостность данных жизненно важна.

Примеры: Центры данных обычно поддерживают данный уровень защиты. Сведения о заработных платах, личном составе, бухгалтерских данных, паролях, информации о слабости корпоративной безопасности, очень конфиденциальные клиентские данные и конфиденциальные контракты.

Строго конфиденциальная информация

Несанкционированный внешний или внутренний доступ к таким данным может иметь огромное значение для компании. Целостность данных имеет жизненно важное значение. Число людей, имеющих доступ к таким данным, должно быть очень невелико. В отношении использования таких данных должны соблюдаться очень строгие правила.

Примеры: Секретные контракты.

Специалисты по информационной безопасности должны определить соответствующие меры защиты, необходимые для каждого классификационного уровня.

Информационные системы, используемые для обработки данных, должны отвечать соответствующим требованиям.

Высшие должностные лица компании несут общую ответственность за реализацию политики безопасности.

Принятая классификация данных должна периодически пересматриваться.

Пример методики категорирования ведомственной информации

Рассмотрим пример методики, учитывающий только конфиденциальность информации.

При определении перечня информации, составляющей коммерческую тайну, необходимо учитывать положения отечественного законодательства, устанавливающего перечень сведений, которые не могут составлять коммерческую тайну.

1 ЭТАП — АНАЛИЗ СИСТЕМЫ КРИТЕРИЕВ

Идентификация информационного ресурса

К1 Название.

К2 Владелец информационного ресурса (подразделение, источник данных).

К3 Категория (категории) субъектов, которым требуется данный информационный ресурс в соответствии с технологией обработки информации.

К4 Категория (категории) субъектов, которым может интересовать данный информационный ресурс для осуществления противозаконной деятельности.

Критерии для оценки негативных аспектов (рисков и затрат), связанных с несвоевременным раскрытием информации

В зависимости от категорий субъектов:

Н1 Возможность прямых (или косвенных) финансовых потерь ОРГАНИЗАЦИИ.

Н2 Возможность негативного общественного резонанса.

Н3 Осложнение отношений с партнерами (подрядчиками, смежниками).

Н4 Использование информации для проведения терактов и актов саботажа.

Н5 Извлечение личных выгод лицом, группой лиц, конкурентами.

Н6 Невозможность своевременного получения информации потенциально заинтересованными партнерами.

Н7 Затраты, связанные с закрытием информации (организационный аспект).

Н8 Затраты связанные с раскрытием информации после истечения срока давности (организационный аспект).

Критерии оценки позитивных аспектов, связанных с незакрытием информации

П1 Возможность извлечения прямых (или косвенных) финансовых выгод.

П2 Возможность позитивного общественного резонанса.

П3 Возможность установления новых партнерских отношений и улучшения отношений с существующими партнерами.

П4 Возможность извлечения выгод (разного рода) другими подразделениями ОРГАНИЗАЦИИ и партнерами.

П5 Улучшение качества решений за счет публичного обсуждения информации.

Каждая из шкал в качественной или номинальной шкале.

С целью упрощения процедуры экспертной оценки рекомендуется использовать шкалы с малым числом градаций.

Примеры шкал критериев

К4: журналисты, собственные (потенциально недобросовестные) сотрудники, террористы, партнеры, конкуренты.

Н1:

- 0 — отсутствие эффекта или незначительный эффект (менее $ 1 000),
- 1 — ощутимый эффект ($ 1 000–50 000),
- 2 — очень значительный эффект (более $ 50 000).

Н2:

- 0 — отсутствие резонанса или незначительный резонанс (кулуарные обсуждения сотрудников негативного характера),
- 1 — ощутимый резонанс (критические публикации в СМИ, не имеющие серьезных последствий и т. п.),
- 2 — очень значительный резонанс (Негативная реакция на уровне думы, правительства, региональных властей, акционеров с оргвыводами).

Н3:

- 0 — отсутствие влияния или незначительное ухудшение качества субподрядных работ для ОРГАНИЗАЦИИ,
- 1 — ощутимое влияние,
- 2 — существенные негативные последствия.

Н4:

- 0 — отсутствие возможности или незначительные неприятности (сбои технологического процесса),

- 1 — возможны неприятности с ощутимыми последствиями,
- 2 — возможны очень крупные неприятности (существенные сбои в технологических процессах, разрушение имущества, жертвы среди сотрудников).

Н5:

- 0 — отсутствие возможности либо возможны незначительные последствия (например, возможно использование информации для интриг и скандалов внутри ОРГАНИЗАЦИИ),
- 1 — возможны ощутимые последствия, (например, осложнить отношения с партнерами),
- 2 — возможны очень серьезные последствия (такие как использование информации для оказания давления на отдельных лиц или структуры ОРГАНИЗАЦИИ, извлечение крупной финансовой выгоды).

Н6:

- 0 — отсутствие влияния либо незначительное влияние,
- 1 — возможны ощутимые последствия (ухудшение качества субподрядных работ для ОРГАНИЗАЦИИ, затруднение инициатив субподрядчиков по внесению изменений, улучшающих качество работ для ОРГАНИЗАЦИИ, и др.),
- 2 — возможны очень серьезные последствия

Н7:

- 0 — отсутствие затрат, либо незначительные затраты,
- 1 — ощутимые затраты (потребуется внесение изменений в регламенты обработки и хранения информации, повышается трудоемкость процедур обеспечения защиты информации),
- 2 — затраты чрезвычайно велики (существенное повышение трудоемкости и стоимости процедур защиты информации, необходимость увеличивать штат для обеспечения режима ИБ).

Н8:

- 0 — отсутствие затрат, либо незначительные затраты,
- 1 — ощутимые затраты (потребуются дополнительные усилия в организационном плане и материальные затраты),
- 2 — затраты чрезвычайно велики (потребуются существенные дополнительные затраты и усилия, необходимо увеличить штат).

П1:

- 0 — отсутствие эффекта или незначительный позитивный эффект,

- 1 — ощутимый эффект ($50 000 — 500 000) (за счет устранения дублирования работ, открытого обмена информацией с партнерами),
- 2 — значительный эффект (Более $ 500 000).

П2:

- 0 — отсутствие позитивного резонанса (или незначительный),
- 1 — ощутимый эффект (позитивные публикации в СМИ, и т. п.),
- 2 — очень существенный эффект (помощь со стороны партнеров, правительства, руководства регионов в достижении целей).

П3:

- 0 — отсутствие позитивного эффекта (или незначительный),
- 1 — ощутимый эффект (возможность получить предложения от потенциальных партнеров по более эффективному решению стоящих перед организацией задач и т. п.),
- 2 — очень существенный эффект (возможность разрешения крупных проблем, осуществление важных проектов и т. п.).

П4:

- 0 — отсутствие позитивного эффекта (или незначительный),
- 1 — ощутимый эффект (упрощение координации работ с партерами, взаимовыгодный обмен информацией, и т. п.)
- 2 — очень существенный эффект (возможность разрешения крупных проблем, осуществление важных проектов и т. п.)

П5:

- 0 — отсутствие позитивного эффекта, (или незначительный),
- 1 — ощутимый эффект (повышение качества технологических решений за счет открытого обмена информацией),
- 2 — очень существенный эффект (возможность разрешения крупных проблем, осуществление важных проектов и т. п.).

2 *ЭТАП — ФОРМИРОВАНИЕ МАТРИЦЫ КЛАССИФИКАЦИИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ*

Предлагается ограничиться 3 категориями:

- Информация 0 категории — Открытая информация. Закрывать не целесообразно.
- Информация 1 категории — Существенная информация. Ее раскрытие нежелательно, хотя эффект от раскрытия может быть не столь велик. Затраты, связанные с закрытием информации, могут быть существенны. Принятие решения об отнесении данной информации к ка-

кой-либо категории (открытая или закрытая) принимается экспертами после дополнительного изучения.

- Информация 2 категории — Критически важная информация. Ее несвоевременное раскрытие может иметь значительные негативные последствия. Такую информацию следует закрывать вне зависимости от связанных с этим затрат.

Отнесение к каждой из категорий производится в зависимости от значений перечисленных выше критериев. Для этого задается матрица (правило), которая позволяет автоматически по значениям критериев относить к той или иной категории определенный информационный ресурс. В простейшем случае правило может быть определено следующим образом:

- **Категория 0** — если критерии Н имеют значение 0 или не более двух любых критериев 1.
- **Категория 1** — если критерии Н имеют значение 0 или 1 (более двух любых критериев 1), критерии П имеют значение 0 и не более 1 критерия — значение 1.
- **Категория 2** — если критерии Н имеют более 3 значений 1 или более 1 значения «2», критерии П имеют значение 0 и не более 1 критерия — значение 1.

Для целого ряда неочевидных случаев, когда имеются высокие значения по негативным (Н) и позитивным (П) критериям, необходимо дополнительно определить правила категорирования с учетом мнений экспертов.

Литература

1. *Quist A. S.* Security Classification of Information. Vol. 2. Principles for Classification of Information U. S. Department of Energe. 1993.
2. Security Classification of Official Information. Instruction 5210.47, Appendix A, Part I / U.S. Department of Defense. Dec. 31, 1964. Hereafter cited as «DoD 5210.47.»
3. EO 12065, Order to specifically identify classifiable NSI areas.
4. *Devadason F. J.* A Methodology for the Identification of Information Needs of Users. 62nd IFLA General Conference — Conference Proceedings — August 25–31, 1996.
5. *Chancellor* DATA CLASSIFICATION POLICY THE UNIVERSITY OF NORTH CAROLINA AT GREENSBORO. 2004.
6. Data Security and Classification Guidelines. Official publication of the University of Massachusetts.
7. Classification Guidelines And Distribution Controls (www.dss.mil/seclib/index.htm). Best practices in data classification for information lifecycle management. White Paper Networked Information Systems.