

2. *Лобанов И.А., Мелихов А.А., Белавкин П.А.* Формирование иерархии синтаксических структур при управлении взаимодействием информационных потоков / Нейрокомпьютеры и их применение: тезисы докладов (13 марта 2018 года Москва). – Москва: Московский государственный психолого-педагогический университет, 2018. – С. 403-405.

---

**Козлов А.Д., Нога Н.Л.**

### **Достоверность информации как элемент обеспечения информационной безопасности и оценка ее уровня**

**Аннотация:** В работе авторы предлагают дополнить основные характеристики обеспечения информационной безопасности информационных систем, включая сложные сетевые структуры, категорией достоверности, как ее важной составляющей.

**Ключевые слова:** достоверность, информационная безопасность, доверие, уровень достоверности, нечеткая логика

В настоящее время в России поставлена задача широкого внедрения цифровых технологий в различных областях экономики [1,2], включая, в том числе, разработку и внедрение систем с искусственным интеллектом.

Федеральная программа «Цифровая экономика Российской Федерации» определяет, что для решения всего комплекса поставленных задач и достижения указанных целей необходимо развитие и совершенствование основных инфраструктурных элементов цифровой экономики (информационная инфраструктура, информационная безопасность).

Нормативные документы в области информационной безопасности (ГОСТы, РД и др.) направлены на защиту информации от несанкционированного доступа, модификации или потери возможности ее использования. Категории защиты, относящиеся к этим трем типам нарушения безопасности, обычно называют конфиденциальностью, целостностью и доступностью.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите

информации» кроме вышеназванных типов нарушения указывает на необходимость обеспечения достоверности в информационных системах. При этом за нарушения принципа достоверности в государственных информационных ресурсах предусмотрена ответственность, вплоть до уголовной.

Так что такое достоверность, как она обеспечивается и как может влиять на результаты функционирования цифровой экономики?

Достоверность информации – свойство информации, характеризующее степень соответствия реальных информационных единиц их истинному значению [3]. Также можно определить, что достоверность информации – это характеристика ее неискаженности. Достоверность информации сильно зависит от ее адекватности, объективности, полноты и полезности.

Полезность информации обеспечивается за счет применения фундаментальных качественных характеристик – уместности, правдивого представления и существенности, и повышается за счет таких качественных характеристик, как сопоставимость, своевременность, проверяемость и понятность [4]. Правдивое (достоверное) представление информации в свою очередь характеризуется полнотой, нейтральностью и отсутствием существенных ошибок.

Как известно, даже в бухгалтерской отчетности нет 100% достоверности, и параллельно может существовать «белая» и «черная» бухгалтерии. Также возможно использование недостоверного (например, похищенного) аккаунта в различных сетевых ресурсах.

Но если недостоверную информацию предоставить для выработки управленческих решений, то результат может быть плачевный. Не говоря о важности достоверных разведанных при проведении военных операций, можно привести следующие повседневные примеры.

Сейчас многие пользуются услугами различных навигаторов: недостоверная информация о дорожной ситуации, ДТП, о поломках городского транспорта может привести к выбору неверного маршрута и потери времени.

В период пандемии важно достоверно знать эпидемиологическую ситуацию в разных регионах: недостоверная

информация может способствовать вспышке заболеваемости или к неоправданно жестким ограничительным мерам.

Особенно важной категория достоверности становится в случаях с искусственным интеллектом – недостоверная информация может привести к невыполнению поставленных задач, а если это связано с системами жизнедеятельности, то и к трагическим последствиям.

Таким образом, достоверность должна являться элементом информационной безопасности.

### **Что влияет на достоверность информации и как ее повысить?**

Для оценки достоверности в информационных системах необходимо проследить всю цепочку от сбора, передачи, обработки, хранения и использования данных, лежащих в основе информационных систем и на основе которых функционирует или будет функционировать цифровая экономика.

#### **1. Сбор данных, какие данные собирает ИС.**

Булевы переменные обладают практически 100% достоверностью, так как могут принимать всего два значения, т.е. характеризовать произошло или нет некоторое событие, подлежащее учету. Такие переменные можно еще назвать – транзакционными, т.к. они могут быть сформированы после завершения некой транзакции.

Количественные переменные. Достоверность количественных переменных зависит от метода их измерения и точности используемого оборудования. Если при этом полученные значения будут суммироваться (например, статистика по регионам), то возможная ошибка будет накапливаться с каждым суммированием.

Качественные переменные являются наиболее субъективными и наименее достоверными.

2. Источник информации и метод сбора. Транзакционный, например, кассовый аппарат в магазине, или сбор статистической или бухгалтерской отчетности по определенным формам за определенный период.

Источник с разным уровнем доверия. При этом низкий уровень доверия может быть компенсирован большим объемом выборки. В этом случае статистическая погрешность уменьшается.

Необходимо учитывать, что «излишняя доверчивость» может привести к отрицательному результату, так как через доверенный источник может также поступать дезинформация (чем часто пользуются мошенники). Доверяй, но проверяй.

3. Метод (способ) передачи информации. Информация может поступать в информационную систему непосредственно по каналам электросвязи и автоматически вводиться в БД системы, а может поступать по каналам электронной почты или почтовой связи. В этом случае ввод информации будет осуществляться вручную или в автоматизированном режиме. Чем меньше людей будет задействовано на этом участке, тем меньше влияние субъективных факторов и выше достоверность.

4. Метод обработки данных, включая алгоритмы обработки. Методы обработки могут зависеть от поставленной задачи. В этом случае, при достоверных данных, если применяются неверные (неправильно была поставлена задача) или ошибочные (человеческий фактор) алгоритмы, то могут быть получены неверные (недостоверные) результаты.

5. Своевременная актуализация данных. Чем выше частота обновления данных, тем более достоверная информация находится в информационной системе.

6. Форма и метод использования данных. Например, на объектах критической информационной инфраструктуры требования к обеспечению достоверности должны быть существенно выше.

Для получения достоверной информации необходимо использовать несколько источников, в том числе и с разным уровнем доверия. Чем выше репрезентативность при получении данных, тем выше достоверность информации в ИС.

Основываясь на вышесказанном, достоверность можно представить, как некую функцию, зависящую от перечисленных параметров.

$$D = D\{TD, \Delta i, K_i, MT, MP, A(t), U\} \quad (1)$$

где TD – параметр, определяющий тип данных;  $\Delta i$  – ошибка измерения;  $K_i$  – параметр, характеризующий источник информации, включая репрезентативность выборки; MT – характеристика метода сбора и передачи информации; MP – характеристика метода

обработки данных;  $A(t)$  – частота обновления (актуализации) информации;  $U$  – характер (цель) использования данных.

### **Оценка достоверности**

Так как категория достоверности является элементом безопасности информационных технологий, то возникает необходимость оценивать уровень достоверности и риски, связанные с обеспечением достоверности.

В приведенной выше формуле многие параметры трудно представить количественно, а их взаимное влияние находится в области неопределенности. Поэтому предлагается оценку уровня достоверности в информационных системах проводить с использованием метода нечеткой логики аналогично оценке риска информационной безопасности, изложенной в работе [5].

Представив достоверность как лингвистическую переменную и, например, определив экспертным путем границы терма (таблица 1), то можно определять уровень достоверности как качественно, так и количественно.

Таблица 1 – Уровни достоверности

№ п/п	Уровень достоверности	Границы терма «Достоверность»
1	Абсолютно ненадежный	0-0,4
2	Ненадежный	0,4-0,6
3	Довольно надежный	0,6-0,9
4	Полностью надежный	0,9-1,00

### **Выводы**

Достоверность информации в информационных системах различного уровня является важным элементом обеспечения безопасности функционирования цифровой экономики. Для ее обеспечения рекомендуется:

- минимизировать использование качественных показателей в информационных ресурсах;
- максимально использовать транзакционный метод сбора данных, постепенно отказываясь от периодической отчетности;

- минимизировать влияние субъективных факторов (участие человека) на подготовку и передачу данных;
- обеспечивать репрезентативность, дублировать поступающую информацию из разных источников;
- по возможности увеличить частоту обновления (актуализации) данных.

#### Литература:

1. Указ Президента Российской Федерации от 7 мая 2018 года № 204 «в редакции 21.07.2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2024 года». – URL: <http://publication.pravo.gov.ru/Document/View/0001201805070038> (дата обращения 11.10.2021).

2. Указ Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года». – URL: <http://publication.pravo.gov.ru/Document/View/0001202007210012?index=3&rangeSize=1> (дата обращения 11.10.2021).

3. Бизнес ПРОСТ, Что такое достоверность информации? Описание и определение понятия. – URL: <https://biznesprost.ru/dostovernost-informacii.html> (дата обращения 30.09.2021).

4. *Арбатская Т.Г.* К вопросу о сущности категории «достоверность» // Международный бухгалтерский учет. – 2015. – № 8. – С. 17-32.

5. *Козлов А.Д., Нога Н.Л.* Риски информационной безопасности корпоративных информационных систем при использовании облачных технологий // Управление риском. – 2019. – № 3. – С. 31-46.

**Сомов С.К.**

### **Проблема оптимизации схемы восстановления разрушенного оперативного резерва данных в распределенных системах**

**Аннотация:** В работе рассмотрена проблема восстановления разрушенных оперативных данных, используемых в распределенной системе, с помощью специального восстановительного резерва. Предложены различные схемы организации процесса восстановления