УДК 528.71
DOI 10.33764/2618-981X-2023-6-15-19

Д. Г. Вавилов[1], С. Н. Новиков[1]*

Алгоритм альтернативной оценки требований к защищенности персональных данных

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: vavilov.d@mail.ru

Аннотация. Оценка требований к защищенности персональных данных является важным этапом в процессе разработки системы обработки данных. Однако, метод оценки на основе уровня защищенности имеет недочеты, которые могут привести к недостаточной защищенности данных. Основной недостаток метода оценки на основе уровня защищенности заключается в том, что он недостаточно учитывает важность количества субъектов персональных данных, обрабатываемых в системе. В связи с этим, предлагается альтернативное решение – определение требований к защищенности персональных данных, опираясь не только на уровень защищенности, но и на иные, целочисленные факторы. Такой подход позволяет учитывать контекст обработки данных и определять требования к защищенности персональных данных более точно. Кроме того, он может помочь разработчикам систем обработки данных выбрать наиболее подходящие меры по защите данных.

Ключевые слова: уровень защищенности, субъекты информации, персональные данные

D. G. Vavilov[1], S. N. Novikov[1]

Alternate Valuation Algorithm Information Processed in Personal Data Information Systems

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: vavilov.d@mail.ru

Abstract. Assessment of requirements for the security of personal data is an important step in the development of a data processing system. However, the method of evaluation based on the level of security has flaws that can lead to insufficient data security. The main disadvantage of the method of assessment based on the level of security is that it does not sufficiently take into account the importance of the number of personal data subjects processed in the system. In this regard, an alternative solution is proposed - the definition of requirements for the security of personal data, based not only on the level of security, but also on other integer factors. This approach makes it possible to take into account the context of data processing and determine the requirements for the security of personal data more accurately. In addition, it can help developers of data processing systems choose the most appropriate data protection measures.

Keywords: level of security, subjects of information, personal data

Введение

Математическая оценка значимости информации в настоящее время определяется исходя из уровня защищенности в соответствии с требованиями следующих нормативно-правовых актов:

– Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ [1];

– Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ [2];

– Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [3].

– Приказ ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [4].

Постановление Правительства РФ N 1119 [3] регламентирует 4 уровня защищенности информационной системы персональных данных (далее ИСПДн), которые устанавливают на основании категории обрабатываемых персональных данных (далее ПДн) и количества субъектов ПДн в рассматриваемой информационной системе. Такой подход означает, что двум одинаковым системам с незначительной разницей в количестве обрабатываемой информации могут быть присвоены разные уровни защищенности. Таким образом, незначительное количество уровней и использованный подход в установлении числа субъектов ПДн [3] обусловливает недостаточную точность в оценке защищенности ПДн. Поэтому подход к оценке защищенности ПДн, применяемый в настоящее время, является в некоторой степени субъективным и недостаточно точным.

В литературе описаны иные предложения оценки угроз информации [5].

На основании вышеизложенного, цель настоящей работы заключается в разработке альтернативного алгоритма оценки требований к защищенности ПДн.

Методы и материалы

Альтернативный метод оценки защищенности информации предлагается представить в виде математической формулы, результатом которой будет являться коэффициент защищенности ПДн (далее – КЗПДн)

Для разработки методики необходимо иметь следующие исходные данные:

– вид субъекта;
– количество субъектов;
– категории ПДн;
– ценность (финансовые потери);
– тип угроз.

За основу математического представления берется уровень защищенности. Идея заключается в том, чтобы исключить недостатки подхода путем наслаивания новых переменных. В первую очередь устанавливается уровень защищенности ИСПДн, опираясь на условные, заранее известные, исходные данные. Определения типа угрозы осуществляется организацией самостоятельно, основываясь на Модели угроз для системы.

Весь процесс будет рассмотрен на примере условной системы с данными, представленными в табл. 1.

Таблица 1

Исходные данные

Субъект	Количество субъектов	Категории ПДн	Тип угроз	Ценность (Финансовые потери в рублях)
Клиент	150 000	Общие	1	750 млн
Сотрудник	75 000	Общие Специальные Биометрические	3	750 млн

Оценка финансовых потерь осуществляли на основе реальной информации, полученной при утечке данных Яндекса [6]. В первую очередь определяли уровень защищенности для каждого субъекта ПДн.

Результаты

ПДн клиентов системы являются общедоступными, количество превышает 100 тысяч, при этом клиенты не являются работниками предприятия. Актуальные для клиентов угрозы относятся к первому типу. На основании Постановления Правительства РФ N 1119 [3] можно сделать вывод, что информацию необходимо отнести ко второму уровню защищенности.

Информация о сотрудниках относится к трем категориям: общедоступная, биометрическая и специальная. Количество субъектов не превышает 100 тысяч, а актуальными являются угрозы 3 типа. Поэтому на основании Постановления Правительства РФ N 1119 [3] делаем вывод, что информация относится к четвертому уровню защищенности.

Следует заметить, что при присваивании уровней защищенности не рассматривался фактор финансовых потерь при утечке. Для коммерческих организаций данный критерий является основополагающим, поэтому для более точной оценки его необходимо учитывать. Взаимосвязь перечисленных факторов может быть представлена в виде математической зависимости (1):

$$k = \frac{S}{m*y} \ , \qquad (1)$$

где S – ценность информации; m – количество субъектов; y – уровень защищенности информации.

Отношение ценности информации к количеству субъектов представляет собой ценность одного субъекта информации. Значение уровня защищенности в данной формуле призвано увеличить значение количества субъектов. При первом уровне защищенности КЗПДн будет равен финансовым потерям утечки информации об одном субъекте ПДн.

Произведем оценку КЗПДн по предлагаемой методике для условной системы, исходные данные которой представлены в таблице 1. Результат вычислений 2500 у. е.

КЗПДн для сотрудников так же 2500 у. е.

Данный показатель более широко и точно определяет характеристику защищенности информации, чем уровень защищенности. Его преимущество заключается в том, что показатель не имеет числовых границ и является универсальным, для предприятий любого масштаба.

Исходные данные изначально задумывались так, чтобы наглядно показать, зависимость КЗПДн от качества и количества информации.

На основании вышеописанной формулы, можно сделать вывод, что значение КЗПДн прямо пропорционально значимости информации.

Обсуждение

Разработанный алгоритм оценки требований к защищенности позволяет шире рассматривать защищенность ПДн, чем уровень защищенности. Однако, для его успешной реализации необходимо провести дополнительные исследования и применить метод оценки к различным предприятиям с уникальными исходными данными. Только тогда можно будет определить средний показатель и дать сравнительную оценку защищенности ПДн для схожих по масштабам систем.

Заключение

Данный метод оценки требований к защищенности является альтернативным подходом к оценке защищенности информации, но его ценность проявится только с течением времени. Если постепенно, в качестве эксперимента вводить КЗПДн в различных организациях и проводить сравнительный анализ, то такая статистика положительно скажется на обеспечении безопасности ПДн.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ: официальный сайт. – Россия. - URL:https://www.consultant.ru/document/cons_doc_law_61801 (дата обращения: 20.03.2023) – Текст: электронный. - Режим доступа: для авторизир. пользователей.

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ: официальный сайт. – Россия. - URL: https://www.consultant.ru/document/cons_doc_LAW_61798 (дата обращения: 20.03.2023) – Текст: электронный. - Режим доступа: для авторизир. пользователей.

3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: официальный сайт. – Россия. - URL: https://www.consultant.ru/document/cons_doc_LAW_137356 (дата обращения: 20.03.2023) – Текст: электронный. - Режим доступа: для авторизир. пользователей.

4. Приказ ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Пра-

вительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»: официальный сайт. – Россия. - URL: http://www.consultant.ru/document/cons_doc_LAW_167862/ (дата обращения: 29.03.2023) – Текст: электронный. - Режим доступа: для авторизир. пользователей.

5. Статья «Метод определения опасности угрозы персональным данным при их обработке в информационной системе» официальный сайт. – Россия. - URL: https://izv.etu.ru/assets/files/sh-tbtvtp-2017_10_p19-26.pdf (дата обращения: 09.04.2023) – Текст: электронный. - Режим доступа: общедоступный.

6. Новостная статья «Суд постановил выплатить 13 пользователям сервиса доставки «Яндекс Еда» по 5 тыс. рублей за утечку персональных данных» официальный сайт. – Россия. - URL: https://habr.com/ru/news/t/698402/ (дата обращения: 29.03.2023) – Текст: электронный. - Режим доступа: общедоступный.