DOI 10.36622/VSTU.2023.26.1.005
УДК 004.046

ИНСТРУМЕНТАРИЙ АВТОМАТИЗИРОВАННОЙ ОЦЕНКИ И РЕГУЛИРОВАНИЯ РИСКОВ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ РАЗМЕЩЕНИИ В ОТЕЧЕСТВЕННЫХ ХРАНИЛИЩАХ

И.А. Моисеев, Л.В. Паринова, Д.А. Нархов

Данная статья посвящена защите скомпрометированных персональных данных пользователей, находящихся в публичном доступе, а также оценке и регулированию рисков нарушения конфиденциальности данных при их размещениях в открытых хранилищах. В основе методики лежит алгоритм защиты и регулирования личных данных пользователя в информационно телекоммуникационной сети «Интернет». В работе представлены способы защиты конфиденциальной информации и методы борьбы с ресурсами, направленными на сбор и неправомерное использование персональной информации, подверженной компрометации со стороны злоумышленника.

Ключевые слова: персональные данные, риск, конфиденциальность, утечки, база данных.

Введение

В ходе цифрового противоборства сбор и хранение больших массивов персональных данных пользователей порождает множество угроз, как материального, так репутационного и юридического характера [1]. Они могут возникнуть в результате утечки, что является одной из причин, по которой предприятиям следует проявлять осторожность при уточнении или использовании имеющихся у них персональных данных своих пользователей. Чем интенсивнее информационно-телекоммуникационные системы (далее - ИТКС) просачивались в жизнь граждан, тем сильнее обострялась эта опасность, с которой можно справиться при помощи государственного регулирования.

К основным причинам кражи персональных данных (ПДн) пользователей в ИТКС среди злоумышленников можно отнести:

- возможность перепродажи ПДн злоумышленникам;
- ПДн пользователя помогут в создании фишингового письмо под конкретную жертву;
- с помощью ПДн пользователя есть возможность получить доступ к его аккаунтам и устройствам, чтобы использовать их в своих целях;
- с помощью ПДн, в том числе аккаунтов, пользователя можно узнать информацию о других пользователях ресурса. Обладая такого вида информацией, злоумышленники могут более точно подобрать механизмы атаки на цель и найти ее.

При защите ПДн пользователей в сети «Интернет» одним из первых шагов является обнаружение данных, находящихся в открытом доступе, с использованием программно-технических средств (ПТС), систематизации и блокирование данных пользователя в открытых ресурсах [2]. В результате риск-анализа ПДн в публичном доступе, будет вынесено решение о том, насколько надежным является сервис, в котором хранятся данные пользователя, а также даны рекомендации по защите своих данных в информационной системе.

Постановка задач на исследование

Основная цель работы состоит в повышение защищенности ПДн российских граждан за счет создания инструментария автоматизированной оценки и прогнозирования динамики рисков утечки и хищения персональной информации, а также регулирование этих рисков путем адекватного угрозам размещения, перемещением и закрытием защищаемых персональных данных в хранилищах [3].

Для достижения поставленной цели необходимо решить следующие задачи.

1. Создать модуль, позволяющий на основе масштабной статистики нарушений конфиденциальности ПДн (через частоту и ущербность их утечек и хищений) осуществить текущий риск-анализ безопасности ПД в хранилищах.

2. Создать модуль, позволяющий на основе выходных данных модуля риск-анализа прогнозировать динамику рисков нарушения конфиденциальности ПДн и выдавать пользователям практические рекомендации по размещению, перемещению и закрытию ПДн в хранилищах.

3. Интегрировать созданные модули с сервисом размещения ПДн пользователей, включая методический и алгоритмический комплекс и подготовку инструкций для пользователя.

Описание методики количественной оценки и регулирования рисков нарушения конфиденциальности информации

В данной методике, оценка рисков реализуется на анализе баз скомпрометированной информации, количестве расходов, вариаций мошеннических схем, угроз применения, значимости данных и вероятности ущерба, с которой они могут быть реализованы.

С учетом обозначенного определения, формируется методический инструментарий для оценки и регулирования уровня риска, который позволит решить связанные с ним определенные задачи управления личными данными клиентов [4].

К основным показателям такой оценки относятся следующие значения:

• количество персональных данных, находящихся в публичном доступе;

• важность скомпрометированных данных;

• вероятность наступление неблагоприятного события;

Для вычисления риска наступления неблагоприятного события, необходимо рассчитать вероятность:

$$p_N = \frac{2N}{N_o(1 + N_o)}, \quad (1)$$

где N – количество скомпрометированных данных,

N_o-общее табличное количество возможных данных.

В свою очередь ущерб равен:

$$U_N = \sum_{K=1}^{N} u_k, \quad (2)$$

где u_k – важность каждого скомпрометированного данного.

Отсюда риск использования ПДн равен:

$$Risk = p_N U_N, \quad (3)$$

где p_N- вероятность наступления риска,

U_N-величина ущерба.

Для вычисления усредненного риска будет использована несколько измененная версия обычной формулы расчета риска. Изменение будет обусловлено закрытием данных и уменьшением общего количества ПДн, необходимых для соответствия специфики работы с персональными данными. Вычисление вероятности риска, после закрытия данных:

$$p_{N^*} = \frac{2N^*}{N_*(1 + N_*)}, \quad (4)$$

где N^* – оставшееся количество скомпрометированных данных после закрытия,

N_* - общее табличное количество возможных данных после закрытия.

Вычисление возможного ущербы после закрытия данных выглядит так:

$$U_{N^*} = \sum_{K=1}^{N^*} u_k, \quad (5)$$

где u_k – важность каждого скомпрометированного данного.

При этом средний риск равен:

$$\overline{Risk} = \sum_{N=1}^{N_*} p_{N^*} U_{N^*}, \qquad (6)$$

где p_N- вероятность наступления риска,

U_N-величина ущерба.

Уровень важности данных, который будет зависит от реализации возможного количества мошеннических схем, используемых злоумышленником для нанесения некоторого материально и психологического ущерба. Имеющееся градация имеет 13 разновидностей данных, позволяющий мошеннику придумать и реализовать наибольшее количество схем, а также идентифицировать пользователя и получить о нем больше сведений для успешной атаки.

Алгоритм оценки и регулирования рисков нарушения конфиденциальности информации

Прогноз состояние кибербезопасности клиента в алгоритме может дать нейросеть, которая будет брать и проводить анализ текущих утечек по критериям (рис. 1):

- кто первоисточник (допустим компания CDEK) и к кому эти данные относятся;
- когда была утечка (дата, месяц, год);
- какие сведения (поля) утекли (допустим ФИО или просто дата регистрации пользователя).

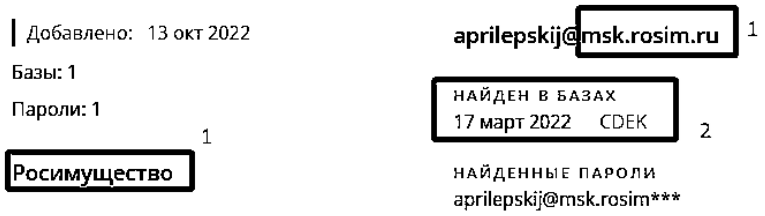

Рис. 1. Пример работы нейросети

Анализ ресурса дает понять, что происходит утечка почты относящийся к Росимуществу. То, что утечка произошла это уже риск. Следующие данные указывают от куда произошла утечка (кто первоисточник) CDEK 17 марта 2022 г.

На основе этих данных, нейросеть запускает процедуру проверки и выполняет следующие действия.

1. Проверка всех утечек связанных с почтами на домене «.rosim.ru».

2. Выведет общее количество фактов утечек по этому домену.

3. Проведет анализ из баз каких организаций они утекли и с какой периодичностью (по датам) (т.е. проведет априорный риск-анализ).

4. Выведет анализ утечек в качестве прогноза: сколько было утечек данных из этой базы в этом году, сколько утечек из этой же базы было в прошлом году.

5. Даст рекомендации для пользователя, что этот ресурс протекает часто и стоит чаще менять пароли или не посещать данный ресурс.

6. Так же даст рекомендации для самой организации на основе компрометации их баз данных.

Разработанное алгоритмическое обеспечение направлено на пресечение неправомерного использование ПДн, находящихся в открытом доступе (рис. 2, 3). Результатом данного алгоритма будет закрытие ПДн в ресурсах путем подачи заявки, а также даны рекомендации по защите своих данных пользователю.

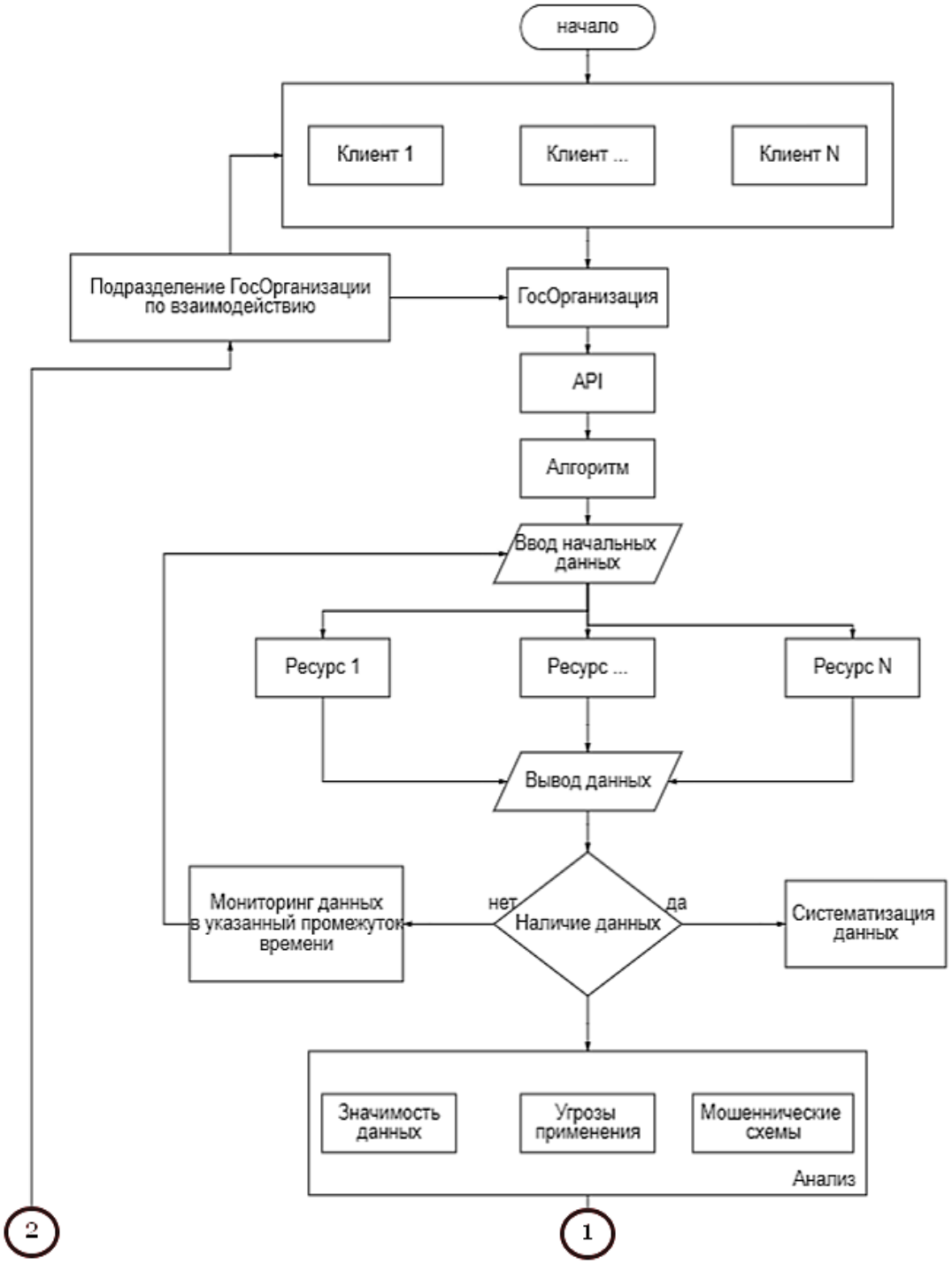

Рис. 2. Алгоритмическое обеспечение безопасности ПДн (начало)

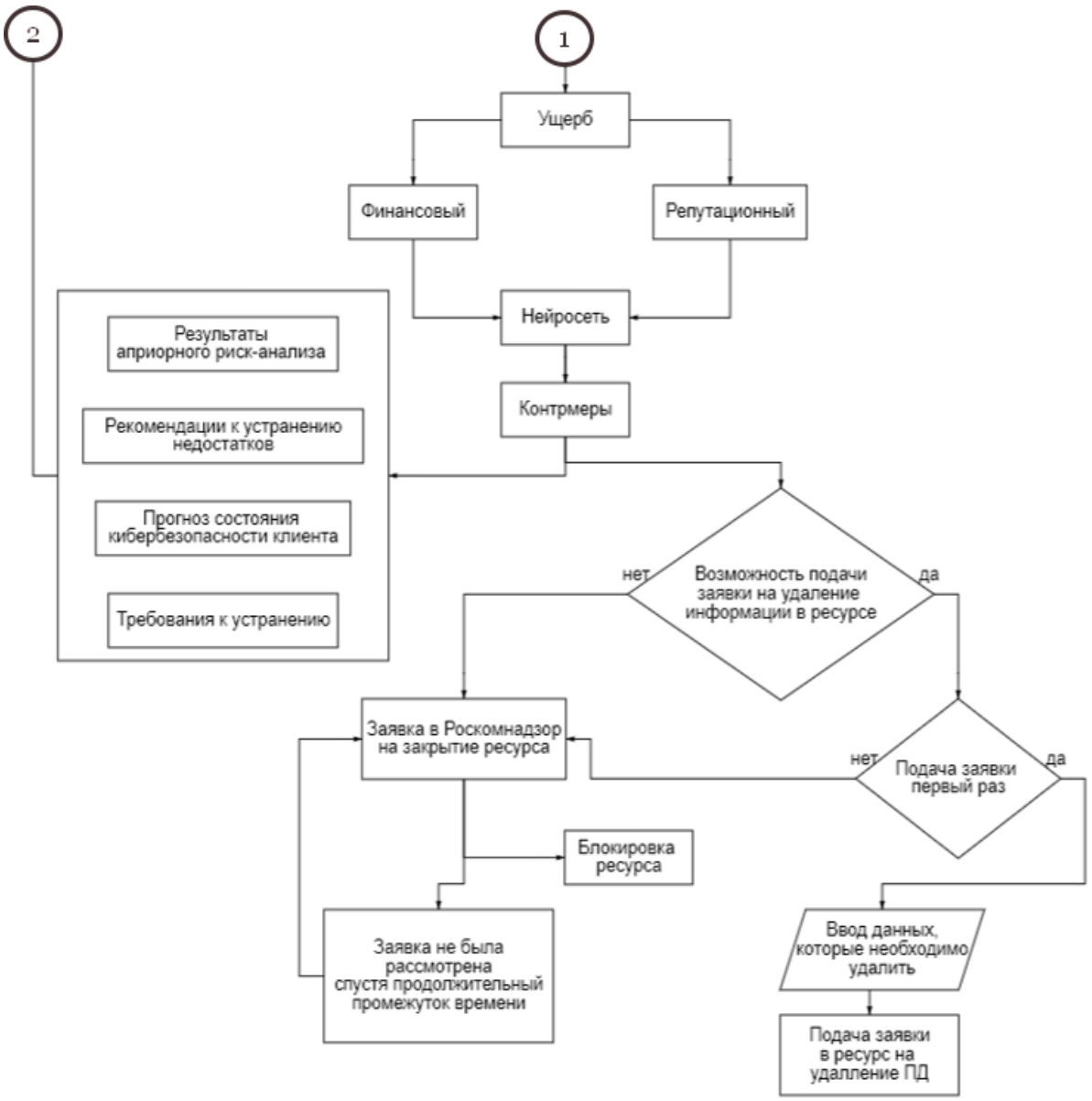

Рис. 3. Алгоритмическое обеспечение безопасности ПДн (окончание)

Заключение

В ходе данной работы, направленной на повышение защищенности персональных данных пользователей в информационно-телекоммуникационной сети, было разработано методическое и алгоритмическое обеспечение, проанализированы исходные данные об утечках информации, также предложены методы по регулированию рисков.

В рамках решения поставленных задач, выявления каналов утечки конфиденциальной информации в информационно-телекоммуникационных сетях, были детально разобраны схемы и способы утечек информации из организаций путем компрометации баз данных клиентов.

Разработанная методика и алгоритм с интегрированными программными модулями оценки и регулирования рисков реализации угроз утечки конфиденциальной информации в ИТКС, в итоге, может быть использована в организациях, деятельность которых связана с информационной безопасностью и ее регулированием.

Список литературы

1. Кафтанникова В.М. Проблемы правового регулирования персональных данных в государственных информационных системах // Проблемы права. 2013. № 2 (40). С. 104-108.

2. Трофимова, И.А. Обработка и хранение персональных данных / И.А.

Трофимова // Делопроизводство.- 2015. № 3. С. 107-110.

3. Губарева А.В., Гулемин А.Н. Угрозы безопасности персональных данных: проблемы современности // Политика и общество. 2015. № 2. С. 151-158.

4. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ URL: http://www.consultant.ru/document/cons_doc_LAW_61801 (дата обращения 18.12.2022).

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 19.02.23

Информация об авторах

Моисеев Иван Алексеевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Паринова Лариса Владимировна – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Нархов Дмитрий Андреевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

TOOLS FOR AUTOMATED ASSESSMENT AND REGULATION OF RISKS OF VIOLATION OF THE CONFIDENTIALITY OF PERSONAL DATA WHEN THEY ARE PLACED IN DOMESTIC REPOSITORIES

I.A. Moiseev, L.V. Parinova, D.A. Narkhov

This article is devoted to the protection of compromised personal data of users in the public domain, as well as the assessment and regulation of the risks of data privacy violations when they are placed in open repositories. The methodology is based on an algorithm for protecting and regulating the user's personal data in the Internet information and telecommunications network. The paper presents ways to protect confidential information and methods of combating resources aimed at collecting and misuse of personal information subject to compromise by an attacker.

Keywords: personal data, risk, confidentiality, leaks, database.

Submitted 19.02.23

Information about the authors

Ivan A. Moiseev – student, Voronezh State Technical University, e-mail: mnac@comch.ru

Larisa V. Parinova – Dr. Sc. (Technical), Professor, Voronezh National Technical University, e-mail: mnac@comch.ru

Dmitrii A. Narkhov – student, Voronezh State Technical University, e-mail: mnac@comch.ru