УДК 004.056

ОЛАДЬКО ВЛАДЛЕНА СЕРГЕЕВНА

РЕШЕНИЕ ЗАДАЧИ ВЫБОРА СРЕДСТВА ВОССТАНОВЛЕНИЯ ДАННЫХ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА ПОЛЬЗОВАТЕЛЯ

АННОТАЦИЯ

В статье рассмотрен подход к принятию решения о выборе предпочтительного средства восстановления данных с машинного носителя. В качестве критерия оптимального средства предлагается использовать максимальное значение аддитивного интегрального показателя оценки по десяти частным критериям. Апробация предлагаемого решения проведена на трех свободно распространяемых средствах восстановления.

Ключевые слова: безопасность информации; машинный носитель; риск; доступность; целостность; аддитивная свертка, принятие решений.

OLADKO V. S.

SOLVING THE PROBLEM OF SELECTING A DATA RECOVERY TOOL

ABSTRACT

The article considers the approach to making a decision on the choice of the preferred data recovery tools from the machine carrier. As a criterion for the optimal tool, author proposed to use the maximum value of the additive integral score for the evaluation according to ten particular criteria. Approbation of the proposed solution was carried out on three freely distributed data recovery tools.

Keywords: information security; the machine carrier; risk; availability; integrity; additive convolution, decision making.

В эпоху массовой цифровизации общества деятельность ни одного человека или организации невозможно представить без применения стационарных и мобильных средств вычислительной техники. Эти средства – автоматизированные рабочие места (АРМ) пользователей, предназначены для хранения, передачи и обработки больших объемов данных, расположенных на физических локальных, съёмных и виртуальных машинных носителях информации. Для выполнения целевых задач и получения пользователями информационных услуг требуемого уровня качества важно в процессе эксплуатации АРМ обеспечить поддержание свойств безопасности информации.

Доступность и целостность информации являются одними из ключевых свойств безопасности информации. В соответствии с ГОСТ Р 50922-2006 [1] доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно. Целостность - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Анализ источников [2,3] показывает, что нарушение доступности и целостности информации может произойти по разным причинам – ошибки пользователя, сбои и отказы про-

граммного или аппаратного обеспечения АРМ, повреждение носителя информации, вредоносное программное обеспечение, несанкционированные действия злоумышленника и как результат – уничтожение информации, ее удаление с носителя, повреждение файлов и прерывание целевых бизнес-процессов. Каждое событие, связанное с нарушением целостности и доступности, влечет риски нарушения непрерывности деятельности и требований безопасности. Значение риска события, связанного с нарушением доступности и целостности данных будет зависть от вероятности реализации события и тяжести его последствий (см. рисунок 1).

Рисунок 1 – Структура системы управления рисками нарушения доступности и целостности

Управление рисками направлено на минимизацию потерь от нарушения целостности и доступности данных, а также сокращение времени простоя системы. Согласно требованиям регулятора, в области информационной безопасности – ФСТЭК России [4], задачи по обеспечению доступности и целостности данных решаются посредством мер, представленных в таблице 1.

Таблица 1.

Меры обеспечения целостности и доступности данных

№	Целевое назначение	Состав мер
1	Обеспечение доступности	Использование отказоустойчивых технических средств. Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования АРМ. Контроль безотказного функционирования технических средств, обнаружение и локализация отказов. Восстановление отказавших средств и их тестирование. Периодическое резервное копирование информации на резервные машинные носители информации. Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала. Кластеризация информационной системы и (или) ее сегментов. Контроль состояния и качества вычислительных ресурсов.

№	Целевое назначение	Состав мер
2	Обеспечение целостности	Контроль целостности программного обеспечения (ПО), включая ПО защиты информации. Контроль целостности информации, содержащейся в базах данных. Обеспечение возможности восстановления ПО при возникновении нештатных ситуаций. Защита от спама. Контроль содержания передаваемой информации. Ограничение прав пользователей по вводу информации Контроль точности, полноты и правильности вводимых данных. Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях

Меры, позволяющие исключить или снизить отрицательные последствия могут носить организационный и технический характер и применяться до наступления негативного события (резервирование данных, введение избыточности и зеркальных сервисов) или после него (процедуры восстановления). Одним из способов восстановления удаленных файлов или данных с поврежденных жестких дисков и других носителей информации является применение специализированных программ восстановления данных. Программы для восстановления данных отличаются своими функциональными возможностями, стоимостью, типами носителей и операционных сред с которыми работают, а также используемыми алгоритмами. Следовательно, решение задачи принятия решений о выборе одного или нескольких альтернативных вариантов решений является достаточно актуальной. Целью исследования является выбор рационального программного средства восстановления данных. Задачей исследования – проведение количественной интегральной оценки программных средств восстановления данных.

Анализ источников [2,5,6] позволил выделить типовые функции, которые реализуются большинством программных средств восстановления данных:

- восстановление удаленных файлов (графических, музыкальных, писем, не сохраненных документов офисных программ);
- восстановление с отформатированных и поврежденных дисков;
- наличие мастера восстановления;
- функция глубокого сканирования файловой системы носителя информации;
- восстановление файлов по сигнатурам.

В общем виде алгоритм поиска потерянных данных и их восстановления можно описать в виде последовательности из четырех шагов на рисунке 2.

Для проведения сравнительной оценки программных средств восстановления данных предлагается использовать взвешенный интегральный показатель, представляющий аддитивную свертку по 10 функциональным и эргономическим критериям (формула 1).

$$Int(prec_j) = \sum_{i=1}^{n} w_i K_i , \qquad (1)$$

где $Int(prec_j)$ – значение интегрального показателя оценки для j-го программного средства восстановления данных из множества анализируемых средств $prec_j \in PREC$; K_i –частный критерий оценки; w_i – вес частного критерия оценки $K_i \in K$, удовлетворяющий условию нормировки $\sum_{i=1}^{10} w_i = 10$.

К функциональным показателям относят целевые функции программного средства, связанные со скоростью и качеством восстановления информации:

- скорость анализа файловой системы носителя информации;
- результативность поиска удаленных файлов;
- скорость восстановления данных;
- количество доступных режимов функционирования;
- нагрузка на производительность ОС АРМ.

Эргономическим являются критерии, связанные с оценкой удобства работы пользователя [7] и его применимостью программного средства к решению поставленной задачи. В работе будут использовать следующие эргономические критерии:

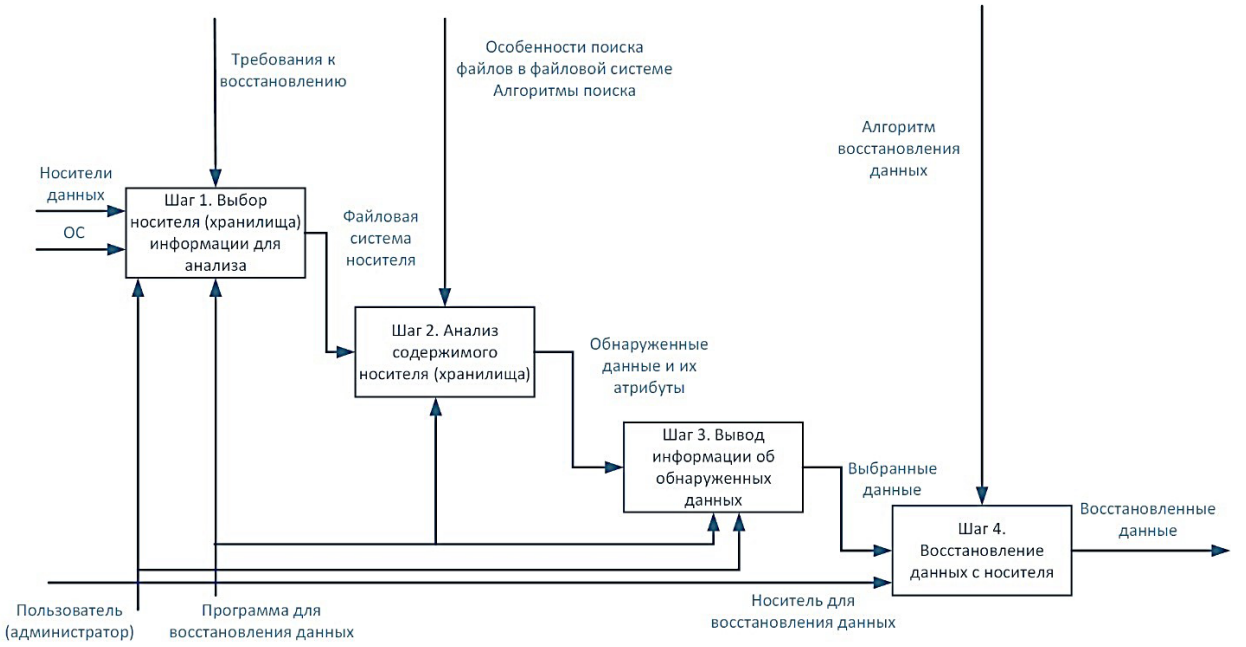

Рисунок 2 – Шаги восстановления данных с носителя информации

– внешний вид интерфейса;
– ”Дружественность” и простота работы с программой;
– скорость установки программы;
– возможность выбора директории поиска;
– полнота и доступность документации.

Часть критериев может иметь качественную, а часть количественную оценку, поэтому для приведения их к общему нормированному значению, предлагается использовать бальную шкалу экспертной оценки от 0 да 10, 0 советует не выполнению критерия средством, 10 – наиболее полное выполнение критерия средством. Предпочтительным $prec^* \underset{Int(prec)}{\mathrm{f}} prec_j$ считается программное средство восстановления данных $prec^* \in PREC$, получившее наибольшее значение интегрального показателя (см. формула 2).

$$prec^* = \arg\max\{Int(prec_j)\ \ prec_j \in PREC\}. \quad (2)$$

Процедура оценки состоит из следующих шагов:

1) определение приоритета важности частных критериев и проверка выполнения суммой критериев условиям нормирования;

2) выбор программного обеспечения для проведения сравнительной оценки по интегральному показателю;

3) определение условий проведения экспериментальных исследований, определение тестового набора файлов, подлежащих восстановлению.

4) установка программного обеспечения и оценка эргономических показателей;

5) проведение экспериментального исследования выбранных программных средств на одной и той же выборки данных, оценка результатов;

6) выставление баллов по частным функциональным и эргономическим критериям;

7) расчет интегрального показателя оценки по формуле 1 для каждого программного средства восстановления данных;

8) сравнение полученных значений интегрального показателя, ранжирование программных и выбор средства с наилучшей оценкой по формуле 2.

Для проведения экспериментального исследования предложенной методики выбора предпочтительного средства восстановления данных на машинном носителе информации было выбрано три альтернативных свободно распространяемых программных средства: Recuva, R.saver и Puran File Recovery. Для проведения эксперимента было использовано 3 машинных носителя информации (локальный носитель, удаленный сетевой диск и съемный USB-накопитель), выборка удаленных файлов насчиты-

вала 100 единиц (30% .docx, 10% .txt, 15% .xls, 35% .jpg, 10% .mp3). Результаты оценки средств по частным критериям представлены в таблице 2 и на рисунке 3.

Таблица 2.

Результаты оценки программных средств восстановления данных

Критерий	*Вес критерия*	*R.Saver*	*Puran File Recovery*	*Recuva*
Внешний вид интерфейс	0.05	10	7	7
Влияние на производительность	0.2	7	10	10
Скорость анализа	0.1	7	10	10
"Дружественность" и простота работы с программой	0.05	10	7	7
Результативность поиска удаленных файлов	0.1	10	10	10
Выбор директории поиска	0.1	5	5	10
Количество доступных режимов функционирования	0.1	1	10	10
Полнота и доступность документации	0.05	5	10	8
Скорость установки	0.05	9	10	10
Скорость восстановления	0.2	7	7	7
	1	71	86	89

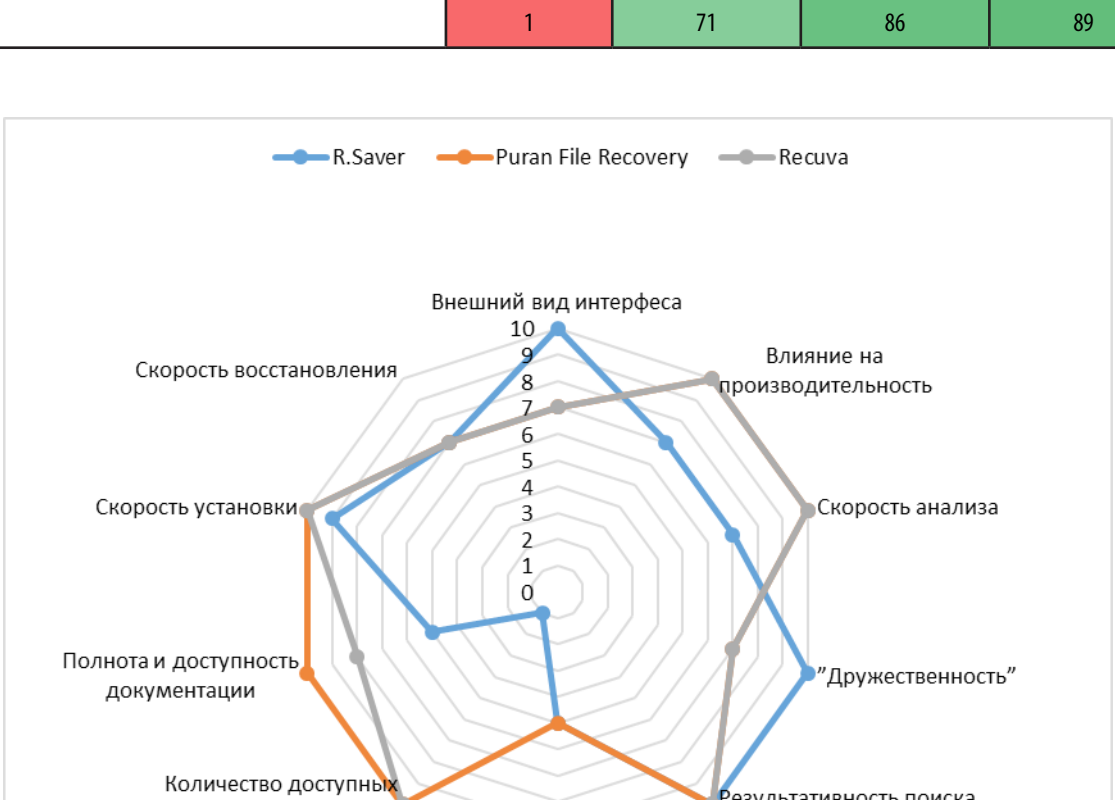

Рисунок 3 – Результаты оценки средств восстановления данных по частным критериям интегрального показателя

Вычисленное значение интегрального показателя указывает, что в данном случае предпочтительным будет являться программное средство Recuva как наиболее полно, из всех альтернатив, удовлетворяющая таким значимым частным критериям как скорость анализа данных машинного носителя, результативность поиска удаленных данных и влияние на производительность АРМ.

Предложенный подход к решению задачи выбора средства восстановления данных с машинного носителя информации АРМ пользователя может использоваться как на практике для формализации принятия решения, так и в учебных целях при формировании профессиональных компетенций студентов, связанных с обоснованием принятых решений по выбору информационных технологий и специализированного программного обеспечения.

Список литературы

1. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения // Электронный фонд правовой и организационно-технической документации [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200058320 (дата обращения 01.07.2018).

2. *Кожевникова И. С., Никишова А. В., Ананьин Е. В., Македонский С. А.* Модель обеспечения целостности данных // Промышленные АСУ и контроллеры. – 2017. – № 4. – С. 34–43.

3. *Оладько В.С.* Управление рисками непрерывности функционирования информационной инфраструктуры организации // Вестник компьютерных и информационных технологий. – 2017. – №1(151). – С. 44–56.

4. Приказ ФСТЭК России «Об утверждении требований по защите информации, не составляющей государственную тайну, содержащийся в государственных информационных системах» // Официальный сайт ФСТЭК России [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (дата обращения 01.07.2018).

5. *Добрынин В. В., Павлиенко А В.* Рынок услуг по восстановлению данных с поврежденных носителей: обзор формирования и развития // Вестник ассоциации вузов туризма и сервиса. – 2009. – № 1. – С.87–95.

6. *Пушкарева А. В., Мясникова М. Г., Цыпин Б. В.* Методика обработки, сжатия и восстановления данных // Измерение. Мониторинг. Управление. Контроль. – 2012. – № 1. – С. 20–25.

7. *Картавенко М. В.* Методология эргономической оценки программного обеспечения в области информационной безопасности // Известия ЮФУ. Технические науки. – 2012. – С.199–204.