Из-за ограничения размера статьи я привела лишь список алгоритмов и существенные особенности, на которые следует обратить внимание [3].

Список литературы

1. Top 10 algorithms in data mining / X. Wu, V. Kumar, J. R. Quinlan et al. Springer-Verlag London Limited. 2007.

2. Top 10 Data Mining Algorithms, Explained [Electronic resource]. URL: https://www.kdnuggets.com/2015/05/top-10-data-mining-algorithms-explained.html (дата обращения: 08.11.2017).

3. *Oza N.*, *Russell S.* Online Bagging and Boosting // Artificial Inteligence and Statistics, 2001.

УДК 004.65

Е. В. Рясов
Научный руководитель: доц. В. Ю. Бердюгин
Южно-Уральский государственный университет, Челябинск

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ИСУБД «CRONOSPRO» ДЛЯ ОРГАНИЗАЦИИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИСПДн

Аннотация. Деятельность по обеспечению информационной безопасности, как и любая другая организационно-управленческая деятельность, нуждается в информационно-аналитическом обеспечении. Формы и методы организационно-управленческой деятельности применяются в определенной последовательности, цикличности, диктуемой интересами и целями подготовки, принятия и исполнения управленческих решений. Этапы управленческой деятельности имеют логическую связь и образуют в совокупности цикл управленческих действий. В качестве объекта исследования выбрана деятельность по обеспечению защиты информационной системы персональных данных (ИСПДн). Для удовлетворения информационных потребностей, возникающих при защите ИСПДн, предлагается использовать инструментальную систему управления базами данных (ИСУБД) «CronosPro».

Ключевые слова: информационная безопасность; персональные данные; инструментальная система; организационно-управленческая деятельность; информационно-аналитическое обеспечение; ИСУБД «CronosPro».

Согласно статье 2 Федерального закона от 28.12.2010 № 390 «О безопасности», одним из основных принципов обеспечения безопасности является системность и комплексность применения мер данной деятельности. При обеспечении безопасности ИСПДн мы также обязаны руководствоваться данным принципом.

Под информационно-аналитическим обеспечением деятельности по защите ИСПДн понимается комплекс организационно-управленческих мероприятий и приемов по изучению и оценке определенной совокупности информации, характеризующей состояние информационной системы, результаты деятельности подразделений информационной безопасности по выполнению стоящих перед ними задач, а также условий, в которых данные задачи решаются.

Исходя из перечня мер, обеспечивающих защиту ИСПДн, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ, постановлении Правительства Российской Федерации от 01.11.2012 № 1119 и приказе Федеральной службы по техническому и экспортному контролю России от 18.03.2013 № 21, сотрудникам подразделения защиты информации необходимо обеспечить:

1. Относительно функции информационной системы по загрузке, хранению и извлечению данных:

- ведение базы данных, содержащих информацию обо всех лицах, взаимодействующих с ИСПДн;
- ведение и поддержку актуального состояния документационного обеспечения системы безопасности ИСПДн;
- учет носителей персональных данных (ПД);
- накопление информации о проведении инструктажа сотрудников;
- учет результатов служебных разбирательств, по фактам нарушения требований информационной безопасности.

2. Относительно функции информационной системы по решению информационно-логических задач:

- учет осведомленности сотрудников организации;
- выявление инцидентов, связанных с нарушениями требований безопасности ИСПДн.
- контроль наличия носителей ПД у сотрудников организации;
- фиксацию взаимодействий организации со сторонними учреждениями (юридическими лицами, органами, осуществляющими контроль защищенности ИСПДн);
- выявление скрытых связей (второго и последующих уровней) при проведении компьютерной экспертизы [1–3].

Определяющей тенденцией в сфере обеспечения информационной безопасности является создание баз данных для автоматизации выполнения требований законодательства Российской Федерации [4].

В частности, когда речь идет об обеспечении информационно-аналитической деятельности по защите ИСПДн большую роль играет выбор СУБД как непосредственной системы обработки защищаемой информации. Необходимо отметить, что к данному инструменту также предъявляются требования соответствия положениям нормативной правовой базы в сфере информационной безопасности.

Нами проведен сравнительный анализ СУБД, располагающих набором соответствующих возможностей, которые представлены в табл. 1.

Таблица 1

Сравнительные характеристики СУБД

Название продукта	Минимальные системные требования	Гибкость настройки	Возможность разработки дополнительных модулей	Наличие встроенных функций анализа данных	Лицензии и сертификаты
Oracle	ОЗУ — 2 ГБ HDD — 3 ГБ ОС Windows server 2008	Зеркалирование данных, импорт и экспорт данных	Присутствует	Нет	Нет
IBM DB2	ОЗУ — 2 ГБ HDD — 1 ГБ ОС Windows/ Linux	Импорт и экспорт данных, резервное копирование	Присутствует	Нет	Нет
1С Документооборот	Зависит от устанавливаемого дистрибутива	Импорт и экспорт данных, резервное копирование	Присутствует	Конструктор отчетов	Сертификат соответствия ФСТЭК
CronosPro	ОЗУ — 256 Мб (для Windows XP) HDD — 15 Мб ОС Windows	Импорт и экспорт данных, резервное копирование	Присутствует	Конструктор отчетов, построение графического отображения связей.	Сертификат соответствия ФСТЭК, лицензии ФСТЭК и ФСБ

В результате нами выбрана ИСУБД [3] «CronosPRO» как наиболее подходящее средство решения поставленной задачи.

Дополнительными преимуществами данной ИСУБД являются:

– возможность адаптации банка данных, созданного для обеспечения безопасности конкретной ИСПДн в случае изменения ее структуры (количества субъектов или категории ПД и т. д.);
– возможность создавать запросы любой сложности;
– использования ИСУБД в правоохранительных органах, деятельность которых по своему содержанию схожа с деятельностью по обеспечению безопасности ИСПДн.

Для решения информационно-аналитических задач сотрудникам подразделения защиты информации нами создан банк данных, который содержит в себе следующие взаимосвязанные базы данных:

– лиц (база данных содержит информацию о сотрудниках нашей организации, и других лицах, взаимодействующих с ИСПДн);
– организаций (она содержит информацию об организациях, взаимодействующих с ИСПДн);
– действий (фиксируются действия лиц, связанные с ИСПДн, служебные разбирательства, факты неправомерного доступа к ИСПДн, действия сотрудников подразделения защиты информации);
– носителей (содержит информацию о носителе ПД, дате ввода и вывода из эксплуатации);
– средств защиты (информацию о средствах защиты ИСПДн).

Разработаны входные формы для ввода информации и библиотека запросов для решения типовых информационно-логических задач.

Список литературы

1. Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3. Приказ ФСТЭК России № 21 от 18.03.2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4. *Мищенко Е. Ю., Соколов А. Н.* Количественный анализ процедуры обезличивания персональных данных. Метод перемешивания // Вестн. УрФО «Безопасность в информационной сфере». 2016. № 3 (21). 30 с.