УДК 004.056.2 + 342.7:004.056 + 005.7:004 Вестник УрФО № 1(27) / 2018, с. 57–62

Бердюгин В. Ю., Рясов Е. В.

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ИСУБД «CRONOSPRO» ДЛЯ ОРГАНИЗАЦИИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИСПДН

В настоящей статье рассматриваются вопросы, связанные с организацией информационно-аналитического обеспечения деятельности по защите автоматизированной информационной системы, обрабатывающей конфиденциальную информацию. 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 «CronosPro». Для иллюстрации возможностей приводится пример учета машинных носителей персональных данных.

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

USAGE OF IDBMS «CRONOSPRO» POSSIBILITIES FOR THE ORGANIZATION OF THE INFORMATION AND ANALYTICAL ASSURANCE ACTIVITY FOR IDBMS PROTECTION

In the given article there are the considered questions connected with the organization of the information and analytical assurance of the information security activity of the automated informational system working with confidential information. As an object of study was chosen the activity for IPBS protection. To satisfy the information needs, arising with IPBS protection, it is offered to use the Instrumental database management system «CronosPro».

Keywords: *information security, personal data, instrumental system, organizational management activity, information and analytical assurance, IDBMS «CronosPro».*

Деятельность по обеспечению информационной безопасности, как и другая организационно-управленческая деятельность, нуждается в информационном обеспечении. Формы и методы организационно-управленческой деятельности применяются в определенной последовательности, цикличности, диктуемой интересами и целями подготовки, принятием и исполнением управленческих решений. Этапы управленческой деятельности имеют логическую связь и образуют в совокупности следующий цикл управленческих действий:

• анализ и оценка управленческой ситуации;

• разработка и принятие управленческого решения;

• планирование исполнения принятых решений (разбиение на этапы, назначение ответственных);

• организация и контроль выполнения принятых решений;

• обобщение результатов проведенной управленческой деятельности, оценка новой (результирующей) управленческой ситуации [1].

Организационно–управленческую деятельность по обеспечению безопасности информационной системы персональных данных (ИСПДн), в соответствии с Федеральным законом «О персональных данных» [2], условно можно разделить на два цикла:

1. До начала эксплуатации информационной системы:

• определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

• применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивают установленные Правительством Российской Федерации уровни защищенности персональных данных;

• применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

• оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

2. После ввода в эксплуатацию информационной системы:

• обучение персонала по работе с информационной системой персональных данных;

• учет машинных носителей персональных данных;

• установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных.

• обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

• восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

• контроль над принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

Перечисленные виды деятельности нуждаются в информационно-аналитическом обеспечении.

Под информационно-аналитическим обеспечением деятельности по защите ИСПДн понимается комплекс мероприятий и приёмов по изучению и оценке определённой 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 постановлении Правительства Российской Федерации от 01.11.2012 № 1119 [3] и приказе Федеральной службы по техническому и экспортному контролю России от 18.03.2013 № 21 [4], специалисту по защите информации необходимо обеспечить:

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.

Относительно функции информационной системы по решению информационно-логических задач:

• учёт 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 при проведении компьютерной экспертизы.

Определяющей тенденцией в сфере обеспечения информационной безопасности является создание баз данных для выполнения требований законодательства Российской Федерации [5].

В частности, когда речь идет об обеспечении информационно-аналитической деятельности по защите ИСПДн большую роль играет выбор системы управления базами данных (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 проведён сравнительный анализ СУБД, располагающих набором соответствующих возможностей, которые представлены в виде таблицы (см. табл. 1).

В результате нами выбрана инструментальная система управления базами данных ИСУБД «CronosPRO» как наиболее подходящее средство решения поставленной задачи, так как ключевыми особенностями системы являются:

• наличие инструментов проектирования структуры банков данных;

• возможность ввода/коррекции данных с использованием настраиваемых пользователем форм или стандартных средств;

• визуализация построения сложных запросов с использованием различных критериев и условий, в том числе по нескольким связанным базам данных;

• поддержка одновременного поиска по множеству информационных массивов;

• возможность создания, хранения и использования шаблонов запросов;

Таблица 1

Сравнительные характеристики СУБД

СУБД / Функции	Линтер	CronosPRO	Oracle MySQL
Оперативное удовлетворение информационных потребителей	+	+	+
Непрерывность процесса отбора и переработки информации	-	+	+
Отсутствие дублирования информации	+	+	+
Контроль корректности информации	-	+	+
Приведение обрабатываемых сведений к общему формату	-	+	+
Фильтрация, агрегирование и актуализация информации	-	+	+
Цена	От 25 000 руб	8500 руб (на 10 лет)	≈ 130 000 руб (на 1 год)
Наличие сертификатов	Министерство обороны РФ, ФСТЭК	ФСБ, ФСТЭК	Отсутствуют

• наличие средств визуального отображения и анализа взаимосвязей между объектами;

• поддержка работы с данными внешних форматов (MS Access, MS Excel, Oracle, XML и др.);

• наличие гибкой системы обеспечения безопасности хранимой информации, выполняющей задачи аутентификации пользователей, разграничения доступа к объектам ИСУБД и регистрации происходящих событий;

• возможность автоматического выполнения ряда операций (ревизии, резервного копирования, оптимизации, индексации и др.) по расписанию или в режиме контроля файлов [6].

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

• лиц;

• организаций;

• действий;

• носителей.

Разработаны входные формы для ввода информации, библиотека запросов для решения типовых информационно-логических задач и инструкции пользования банком данных.

В качестве примера рассмотрим организацию информационно-аналитического процесса по учету машинных носителей ПД.

В тексте, при построении алгоритма, используются следующие сокращения, обозначения, символы:

О – ответственный;

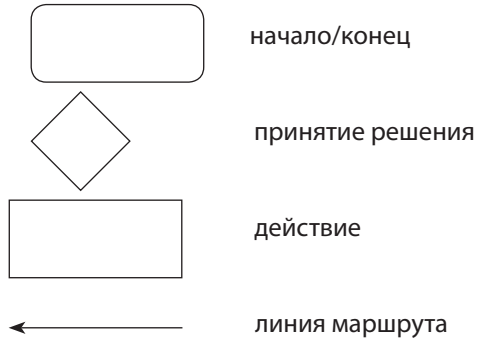
И – исполнитель;

У – участник;

Рук – руководитель организации;

Сотр – сотрудник организации;

Спец – специалист по защите информации в организации.



1. Рук, на основании предложения от Сотр, принимает решение о регистрации носителя.

2. Носитель регистрируется Спец, который вносит информацию в БД.

3. Спец выдает Сотр носитель, факт выдачи фиксируется в БД.

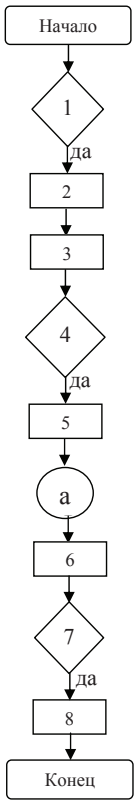
4. При возникновении необходимости передачи носителя от Сотр 1 к Сотр 2, Рук, на основании предложения Сотр 1, принимает решение о передаче.

5. После получения разрешения Сотр 1 сдает носитель Спец, который выдает носитель Сотр 2, о чем делается запись в БД.

6. При необходимости уничтожения носителя Сотр выходит с соответствующим предложением к Рук, который принимает решение об уничтожении носителя.

Таблица 2

Алгоритм действий



Действия	О	И	У
1. Принятие решения о регистрации носителя (1)	Рук.	Спец.	Сотр.
2. Регистрация носителя (2)	Спец.	Спец.	Сотр.
3. Выдача носителя (3)	Спец.	Спец.	Сотр.
4. Принятие решения о передаче (4)	Рук.	Сотр. 1	–
5. Прием носителя (5)	Спец.	Сотр. 1	–
6. Выдача носителя (5)	Спец.	Сотр. 2	–
7. Принятие решения об уничтожении носителя (6)	Рук.	Сотр.	Сотр.
8. Уничтожение носителя (7,8)	Рук.	Спец.	Сотр .1 Сотр. 2

7. Сотр сдает носитель Спец, после чего создается комиссия, составляется акт уничтожения, утверждаемый Рук.

8. Комиссия производит уничтожение носителя, в БД Спец заносит информацию о выведении носителя из работы.

БД лиц формируется из руководителя, специалиста и сотрудников организации. БД действий формируется из регистрации, выдачи, приема и уничтожения носителя. БД носителей формируется из электронных носителей информации (CD, DVD, Blu-ray диски; флэш-память, SSD-диски, дискеты, жесткие диски). Все процессы, связанные между собой, происходят в одной организации. Лица будут являться участниками действий, которые происходят с носителем, который в каждый момент времени закреплён за конкретным лицом.

Таким образом, в информационно-аналитической системе будет накапливаться структурируемая информация, которая поможет решать следующие информационно-справочные и информационно-логические задачи:

- накапливать информацию о количестве носителей конфиденциальной информации;
- определять наличие их у сотрудников организации;
- устанавливать количество выведенных из работы носителей.

В результате в любой момент можно получить информацию о том, какое количество сотрудников работало с определённым носителем, и наоборот, с какими носителями работал каждый сотрудник.

Подобным образом, будет функционировать система по отношению к остальным мерам защиты ИСПДн. Построение БД с использованием одних и тех же взаимосвязанных информационных объектов поможет специалисту по защите информации решать сложные информационно-аналитические задачи в том числе выявлять скрытые связи между объектами.

Литература

1. Организация государственного управления – стадии управленческой деятельности. Экономическая энциклопедия. Российская библиотека. – URL: http://economedu.ru/gosupravlenie/159-oraganizacia-upravlenia.html?start=17 (дата обращения: 04.09.2017);

2. О персональных данных: Федеральный закон № 152-ФЗ от 27.07.2006 (с изм. и доп.). – URL: http://www.consultant.ru/document/cons_doc_LAW_61801 (дата обращения: 09.11.2017);

3. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства № 1119 от 01.11.2012 (с изм. и доп.). – URL: http://www.consultant.ru/document/cons_doc_LAW_137356 (дата обращения: 09.11.2017);

4. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК России № 21 от 18.03.2013 (с изм. и доп.). – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 09.11.2017);

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

6. ИСУБД «CronosPRO» URL: http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:CronosPRO (дата обращения: 11.09.2017).

References

1. Organizatsiya gosudarstvennogo upravleniya – stadii upravlencheskoy deyatel'nosti. Ekonomicheskaya entsiklopediya. Rossiyskaya biblioteka. URL: http://economedu.ru/gosupravlenie/159-oraganizacia-upravlenia.html?start=17 (data obrashcheniya: 04.09.2017).

2. O personal'nykh dannykh: Federal'nyy zakon № 152-FZ ot 27.07.2006 (s izm. i dop.). URL: http://www.consultant.ru/document/cons_doc_LAW_61801 (data obrashcheniya: 09.11.2017).

3. Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh: Postanovleniye Pravitel'stva № 1119 ot 01.11.2012 (s izm. i dop.). URL: http://www.consultant.ru/document/cons_doc_LAW_137356 (data obrashcheniya: 09.11.2017).

4. Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh: Prikaz FSTEK Rossii № 21 ot 18.03.2013 (s izm. i dop.). URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (data obrashcheniya: 09.11.2017).

5. Mishchenko Ye.YU., Sokolov A.N. Kolichestvennyy analiz protsedury obezlichivaniya personal'nykh dannykh. Metod peremeshivaniya // Chelyabinsk: Vestnik UrFO «Bezopasnost' v informatsionnoy sfere» № 3(21), 2016. 30 s.

6. ISUBD «CronosPRO» URL: http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:CronosPRO (data obrashcheniya: 11.09.2017).

БЕРДЮГИН Владимир Юрьевич, доцент кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: bvu55@mail.ru.

РЯСОВ Евгений Владимирович, студент кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: Ryasov_zheny@mail.ru.

BERDYUGIN Vladimir, docent of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76,Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: bvu55@mail.ru.

RYASOV Evgeniy, student of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: Ryasov_zheny@mail.ru.