ИНФОРМАТИКА

Вестник Сыктывкарского университета.
Серия 1: Математика. Механика. Информатика.
Выпуск 2 (35). 2020

УДК 004.4/004.5/004.021

ТЕХНОЛОГИИ УПРАВЛЕНИЯ ДАННЫМИ ПРИ ПРОЕКТИРОВАНИИ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

С. Н. Федирко

Рассматриваются информационный менеджмент и технологии управления данными при разработке специализированных систем поддержки принятия решений на основе бесплатно распространяемого программного обеспечения.

Ключевые слова: СППР, безопасность, риски, ITIL, информационный менеджмент.

Существует множество решений, позволяющих обеспечивать приемлемый уровень информационной безопасности в организации, но зачастую они отличаются дороговизной или сложностью сопровождения. Между тем пренебрежение вопросами безопасности может привести к более тяжёлым последствиям, нежели расходы на приобретение и внедрение комплексного решения.

Чтобы сохранить баланс между ценой и качеством обеспечения состояния защищённости, организация может воспользоваться собственными разработками, основанными на продуктах, доступных в открытом доступе. Таким образом, стоимость подобного решения будет существенно ниже, чем у востребованных на рынке аналогов [1].

Одним из подобных решений может являться некая система поддержки принятия решений (СППР), основанная исключительно на рассматриваемой организации. В таком случае основной задачей будет её грамотное обучение и наполнение баз, с которыми СППР будет взаимодействовать.

Чтобы спроектировать и смоделировать эффективную систему, необходимо использовать качественные технологии, распространённые и хорошо зарекомендовавшие себя мировые практики управления IT-инфраструктурой, а также надёжные источники данных.

Таким образом, целью данного исследования является создание эффективной СППР для поддержания состояния информационной безопасности организации.

Задачи исследования: применить технологии управления данными для планирования системы поддержки принятия решений, поставить гипотезу об эффективности СППР и провести эксперимент с целью её подтверждения или опровержения.

Основная гипотеза эксперимента гласит: создание СППР на основе бесплатно распространяемого программного обеспечения является эффективным средством обеспечения информационной безопасности, значительно уменьшая количество затрагиваемых денежных ресурсов организации (средства, потраченные на стимулирование работников, ответственных за проектирование СППР, намного меньше тех, что организация была бы вынуждена потратить на готовое решение).

Существуют две альтернативные гипотезы:

— Альтернативная гипотеза № 1 — создание СППР на основе бесплатно распространяемого программного обеспечения является эффективным средством обеспечения информационной безопасности, однако затрагиваемые денежные ресурсы организации при её создании больше тех, что предприятие могло потратить на покупку готового решения. Данная гипотеза частично подтверждает основную, и в случае её доказательства поднимается вопрос о сокращении расходов на разработку программного решения.

— Альтернативная гипотеза № 2 — создание СППР на основе бесплатно распространяемого программного обеспечения не является эффективным средством обеспечения информационной безопасности. В случае наступления данной гипотезы количество потраченных средств не имеет значения, так как такое решение нецелесообразно вводить в эксплуатацию. В случае подтверждения данной гипотезы эксперимент считается неуспешным, а представленное решение не принимается в разработку и эксплуатацию.

Эксперимент будет проводиться путём применения востребованных технологий управления данными на этапе планирования, а также методом настройки информационных потоков для функционирования баз данных системы на этапе моделирования.

Основными этапами создания СППР являются: планирование, моделирование и внедрение. Именно они на выходе и будут оцениваться с целью выявления целесообразности предложенного решения. Итогом эксперимента будет являться подсчёт общих затрат на перечисленные процессы относительно СППР в сравнении с покупкой готового реше-

ния.

Диаграмма Ганта [2] показывает временные промежутки, отведённые на выполнение тех или иных этапов (см. рис. 1).

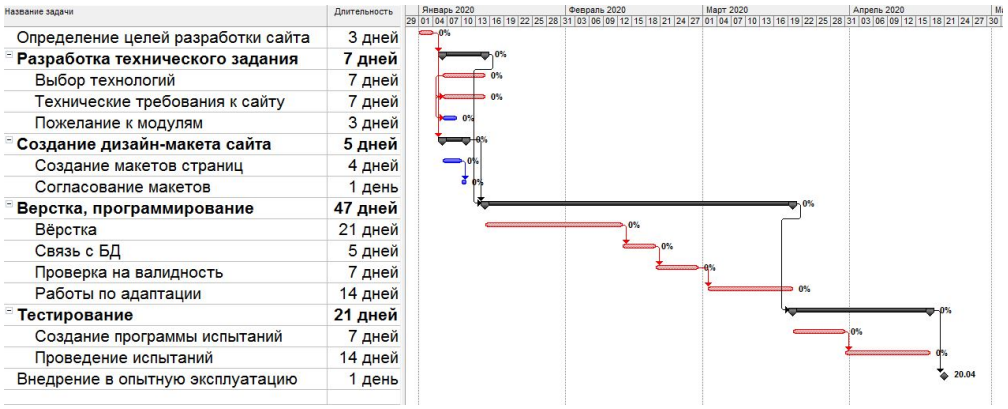


Рис. 1. Диаграмма Ганта для построения СППР

Планирование услуги проще всего представить через модель Дж. Захмана (см. рис. 2, 3) [3]. Через неё можно увидеть, каким будет выглядеть продукт для каждого уровня разработки без отрыва от «холистической» перспективы (взгляда на предприятие как на целое). Основным правилом заполнения данной модели является категорическое исключение «перепрыгивания» через уровни абстракции. Именно последовательное рассмотрение каждого аспекта приведёт к оптимальным решениям как в плане производительности, так и стоимости реализации (целью чего и является сама идея СППР).

Так как в данном случае одним из основных критериев создания СППР является экономия денежных ресурсов стороны организации, в качестве СУБД была выбрана MySQL [4] — свободная реляционная система управления базами данных.

После этапа планирования системы необходимо перейти к этапу её моделирования, ключевым процессом которого является формирование информационных потоков данных, на которые будет ссылаться СППР. Основными источниками анализируемой информации являются:

— банк данных угроз безопасности информации ФСТЭК России [5]. Данные представлены в формате CSV-таблиц, пригодных для обработки в MySQL;

— банк данных уязвимостей согласно ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [6];

Уровень абстракции		Миссия (Зачем?)	Партнёры (Кто?)	События (Когда?)
Заказчик	Цели и сфера бизнеса	Обеспечение состояния информационной защищённости	Сотрудники ПФР	В любой момент времени функционирования органа ПФР
	Бизнес-модель предприятия	Защита конфиденциальности, целостности, доступности данных	• Управляющий • Заведующий направлением • Начальник отдела • Специалист (согласно перечню ИОД)	Сроки обработки конфиденциальной информации
Проектировщик	Логическая модель	• Управление рисками • Создание модели угроз • Создание модели нарушителя	• Пользователи • Администраторы • Ревизоры	• Появление новых угроз и уязвимосте • Создание новых отделов • Появление новой информации
Разработчик	Техническая инфраструкту-	• Управление архитектурой	• Разработчик • Проектировщик	• Инцидент • Проблема

Рис. 2. Фрагмент модели Захмана для СППР. Часть 1

Уровень абстракции		Данные (Что?)	Функции (Как?)	Сеть (Где?)
Заказчик	Цели и сфера бизнеса	Информационная безопасность	• Обеспечение • Устранение уязвимостей • Проактивное управление	Республика Коми
	Бизнес-модель предприятия	• Угрозы • Уязвимости Активы • Отделы	• Мониторинг событий ИБ • Формирование безопасной среды	• Отделение ПФР • Управления ПФР • Центр ВП • Клиентские службы
Проектировщик	Логическая модель	• Перечень угроз ФСТЭК • ГОСТ Р 27005-2010 • Перечень отделов • Перечень сотрудников • Перечень активов • Перечень ИОД	• Сортировка • Выборка • Корректировка данных в условиях рассматриваемой организации	• Абонентские пункты • Пользователи ИС • Администраторы ИС
Разработчик	Техническая инфраструктура	• Базы данных • CSV - таблицы	• SQL – запросы • Скрипты AutoIT	• Протокол TCP • Протокол MySQL

Рис. 3. Фрагмент модели Захмана для СППР. Часть 2

— документация организации в области организационной структуры и сведения о бизнес-процессах. Данная информация необходима для создания блоков «Отделы» и «Активы» системы. В зависимости от иерархического уровня организации данные блоки могут изменяться, поэтому их наполнение происходит исключительно вручную.

Следующей фазой является анализ данных. Необходимо создать промежуточные таблицы для создания связей «многие ко многим». Важно упомянуть, что данный этап создания системы — самый затратный по времени. Количество связей может достигать нескольких сотен и даже тысяч. Если этого не сделать, система поддержки принятия решений не сможет выдавать адекватные рекомендации на пользователь-

ские запросы. Чем полнее расставлены связи и чем больше внимания уделено сортировке и группировке данных, тем эффективнее получится система.

Данные будут существовать в формате обыкновенных CSV-таблиц, распознаваемых не только инструментами OpenServer, но и инструментами визуализации данных, таких как Gephi [7], для выполнения кластерного анализа, если это необходимо.

Последней фазой создания СППР является написание интерфейса (рис. 4). Данные хранилища решено обрабатывать с помощью скриптового языка PHP [8]. Для отображения данных будет использоваться язык гипертекстовой разметки HTML с использованием CSS. Динамику системе придаст jQuery (библиотека JavaScript), а визуальное оформление — HTML, CSS, JS фреймворк Bootstrap [9].

Выбирая из четырех доступных групп: «Уязвимости», «Угрозы», «Отделы» и «Активы», можно получить точки пересечения, которые были созданы на стадии наполнения хранилища данных. В зависимости от того, какие совпадения в системе нашла СППР, она будет давать рекомендации по их устранению. Также она выводит вероятности использования уязвимостей, чтобы пользователю было понятно, чем нужно заняться в первую очередь, а что можно отложить.

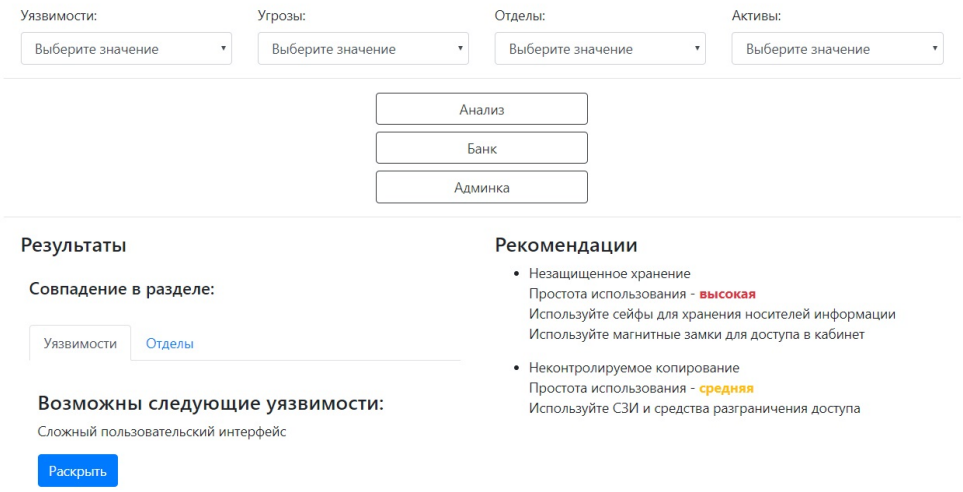


Рис. 4. Интерфейс пользователя СППР

Внедрение системы выполняется на антивирусном сервере организации путём развёртывания базы данных и назначения ip-адреса. Также подготавливается приказ о вводе в эксплуатацию и письмо руководите-

лям структурных подразделений Отделения и начальникам нижестоящих филиалов.

Как было сказано выше, итогом эксперимента будет сравнение потраченных на СППР ресурсов организации со стоимостью готовых решений.

Для определения стоимости готового решения был произведён анализ наиболее популярных решений на рынке, предлагаемых компаниями, специализирующимися на предоставлении услуг в области обеспечения информационной безопасности [10]. На основе 50 решений подсчитана средняя стоимость построения элементарной системы защиты в этой области — 86800 рублей за год использования. Полноценные же системы мониторинга с продвинутыми инструментами реагирования на события и системы комплексной защиты имеют в разы большие стоимости.

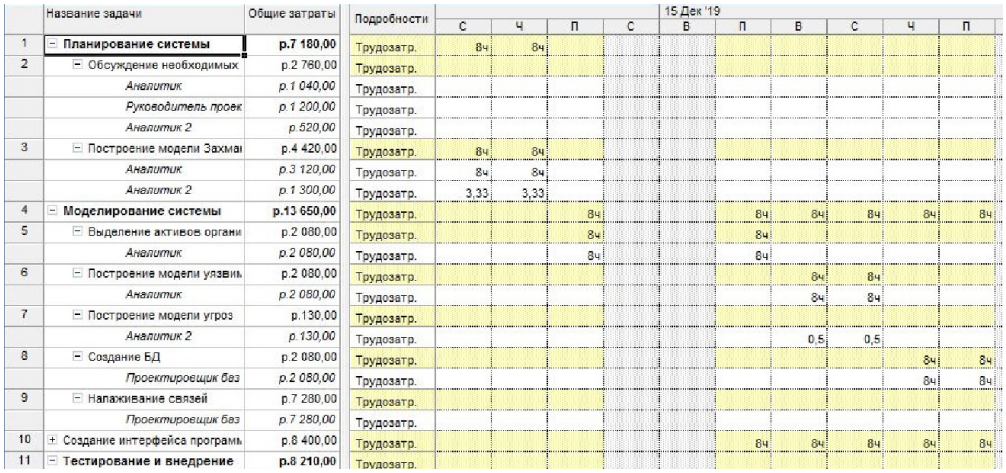
Возможным решением вопроса мониторинга событий ИБ будет несохранение практики проведения систематических аудитов по обеспечению информационной безопасности. Они стоят дешевле, чем готовые решения, однако эта выгода присутствует лишь в краткосрочной перспективе ввиду повторяемости действий по аудиту. Стоимость операций аудита рассчитана на основе прайс-листа услуг по обеспечению информационной безопасности компании Brevis [11].

Таким образом, выполняемые спроектированной системой функции можно выполнить в процессе аудита чуть более чем за 36000 рублей.

Поскольку СППР разрабатывалась на основе бесплатно-распространяемого программного обеспечения, бюджет организации не тратился на лицензии. Единственной статьёй расходов является оплата рабочих часов группы рабочей группы. Модель расчёта расходов проще всего представить через модель Ганта.

Из рис. 5 видим, что затраты на создание СППР составляют 34050 рублей, что меньше, чем стоимость готового решения и аудитов системы. Стоит отметить, что эти затраты единовременны, ведь сопровождение системы будет осуществляться в фоновом режиме путём выдачи роли администратора определённому сотруднику. Более того, выявленная сумма выплачивается за часы, которые сотрудник в любом случае проводит на рабочем месте, сверхурочные выплаты исключены. Таким образом, чистые расходы на создание СППР практически равны нулю.

В ходе данного эксперимента была полностью подтверждена основная гипотеза. Было доказано, что затраты на создание собственной СППР для мониторинга событий информационной безопасности прак-



	Название задачи	Общие затраты	Подробности	15 Дек '19									
				С	Ч	П	С	В	П	В	С	Ч	П
1	**Планирование системы**	**р.7 180,00**	Трудозатр.	8ч	8ч								
2	Обсуждение необходимых	р.2 760,00	Трудозатр.										
	Аналитик	*р.1 040,00*	Трудозатр.										
	Руководитель проек	*р.1 200,00*	Трудозатр.										
	Аналитик 2	*р.520,00*	Трудозатр.										
3	Построение модели Захма	р.4 420,00	Трудозатр.	8ч	8ч								
	Аналитик	*р.3 120,00*	Трудозатр.	8ч	8ч								
	Аналитик 2	*р.1 300,00*	Трудозатр.	3,33	3,33								
4	**Моделирование системы**	**р.13 650,00**	Трудозатр.			8ч			8ч	8ч	8ч	8ч	8ч
5	Выделение активов органи	р.2 080,00	Трудозатр.			8ч			8ч				
	Аналитик	*р.2 080,00*	Трудозатр.			8ч			8ч				
6	Построение модели уязви	р.2 080,00	Трудозатр.							8ч	8ч		
	Аналитик	*р.2 080,00*	Трудозатр.							8ч	8ч		
7	Построение модели угроз	р.130,00	Трудозатр.										
	Аналитик 2	*р.130,00*	Трудозатр.							0,5	0,5		
8	Создание БД	р.2 080,00	Трудозатр.									8ч	8ч
	Проектировщик баз	*р.2 080,00*	Трудозатр.									8ч	8ч
9	Налаживание связей	р.7 280,00	Трудозатр.										
	Проектировщик баз	*р.7 280,00*	Трудозатр.										
10	Создание интерфейса програм	р.8 400,00	Трудозатр.						8ч	8ч	8ч	8ч	8ч
11	**Тестирование и внедрение**	**р.8 210,00**	Трудозатр.										

Рис. 5. Затраты на создание СППР

тически равны нулю при отсутствии сверхурочных часов, а значит, подобные системы являются эффективным средством, позволяющим не только повысить производительность отдела защиты информации, но и сэкономить бюджет организации.

Обосновывается, что данная система — одно из оправданных решений проблемы нехватки инструментов для обеспечения информационной безопасности в организации, исключающее проблемы информационной перегрузки оператора, компенсирующее нехватку его знаний и основанное на бесплатно распространяемом программном обеспечении.

Список литературы

1. **Вишняков Я. Д., Радаев Н. Н.** Общая теория рисков. М.: Издкий центр «Академия», 2008. 368 с.

2. **Кларк У.** Графики Гантта. Учёт и планирование работы. М.: Техника управления, 1931.

3. The Concise Definition of The Zachman Framework by: John A. Zachman [Электронный ресурс] // *Zachman International. URL: https://zachman.com/about-the-zachman-framework (дата обращения: 20.12.2019).*

4. MySQL [Электронный ресурс] // *MySQL. URL: https://www.mysql.com (дата обращения: 20.12.2019).*

5. Банк данных угроз безопасности информации [Электронный ресурс]. URL: https://bdu.fstec.ru (дата обращения: 20.12.2019).

6. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М.: Стандартинформ, 2011. 51 с.

7. The Open Graph Viz Platform [Электронный ресурс] // *Gephi. URL: https://gephi.org (дата обращения: 20.12.2019).*

8. **Веллинг Л., Томсон Л.** Разработка веб-приложений с помощью PHP и MySQL. М.: Вильямс, 2013. 848 с.

9. Bootstrap [Электронный ресурс]. URL: https://getbootstrap.com (дата обращения: 20.12.2019).

10. Network Security Software [Электронный ресурс] // *Capterra. URL: https://www.capterra.com/network-security-software (дата обращения: 20.12.2019).*

11. Лаборатория безопасности [Электронный ресурс] // *Brevis. URL: http://www.brevis-lab.ru/price (дата обращения: 20.12.2019).*

Summary

Fedirko S. N. Data management technologies in designing a decision making support system

Information management and data management technologies are considered during the development of specialized decision support systems based on free software.
Keywords: DSS, safety, risks, ITIL, information management.

References

1. **Vishnyakov Y. D., Radaev N. N.** *Obshchaya teoriya riskov* (General risk theory), M.: Publishing Center «Academy», 2008, 368 p.

2. **Clark W.** *Grafiki Gantta. Uchot i planirovaniye raboty* (Gantt Charts. Accounting and work planning), Moscow: Control Engineering, 1931.

3. The Concise Definition of The Zachman Framework by: John A. Zachman [Electronic resource], Zachman International, URL: https://zachman.com/about-the-zachman-framework (date of the application: 20.12.2019).

4. MySQL [Electronic resource], MySQL. URL: https://www.mysql.com (date of the application: 20.12.2019).

5. Bank dannykh ugroz bezopasnosti informatsii (Databank of information security threats) [Electronic resource], URL: https://bdu.fstec.ru (date of the application: 20.12.2019).

6. *GOST R ISO / MEK 27005-2010. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska informatsionnoy bezopasnosti* (GOST R ISO / IEC 27005-2010. Information technology. Security methods and tools. Information Security Risk Management), M.: Standartinform, 2011, 51 p.

7. The Open Graph Viz Platform [Electronic resource], Gephi. URL: https://gephi.org (date of the application: 20.12.2019).

8. **Welling L., Thomson L.** *Razrabotka veb-prilozheniy s pomoshch'yu PHP i MySQL* (Web Application Development Using PHP and MySQL), M .: Williams, 2013, 848 p.

9. Bootstrap. [Electronic resource], Bootstrap. URL: https://getbootstrap.com (date of the application: 20.12.2019).

10. Network Security Software [Electronic resource], Capterra. URL: https://www.capterra.com/network-security-software (date of the application: 20.12.2019).

11. Laboratoriya bezopasnosti (Security Laboratory) [Electronic resource], Brevis. URL: http://www.brevis-lab.ru/price (date of the application: 20.12.2019).

Для цитирования: Федирко С. Н. Технологии управления данными при проектировании системы поддержки принятия решений // *Вестник Сыктывкарского университета. Сер. 1: Математика. Механика. Информатика. 2020. Вып. 2 (35). С. 59–68.*

For citation: Fedirko S. N. Data management technologies in designing a decision making support system, *Bulletin of Syktyvkar University. Series 1: Mathematics. Mechanics. Informatics*, 2020, 2 (35), pp. 59–68.

СГУ им. Питирима Сорокина *Поступила 25.12.2019*