Источник: Информационные управляющие системы и компьютерный мониторинг 2013 (ИУС и КМ – 2013) / Материалы IV международной научно-технической конференции студентов, аспирантов и молодых ученых. – Донецк, ДонНТУ – 24-25 апреля 2013.

УДК 007.3

АНАЛИЗ МЕТОДОВ ОЦЕНКИ ЗАЩИЩЕННОСТИ КОРПОРАТИВНЫХ СИСТЕМ НА ОСНОВЕ СИСТЕМЫ ГРИФ

Коханова Ю.И., Личканенко И.С., Губенко Н.Е.
Донецкий национальный технический университет
кафедра компьютерных систем мониторинга

Аннотация

Коханова Ю.И., Личканенко И.С., Губенко Н.Е. Анализ методов оценки защищенности корпоративных систем на основе системы «ГРИФ».*Рассмотрена актуальность управления информационной безопасностью на предприятии, а также анализа рисков и угроз на примере частной клиники «Семья+». Определены требования к обеспечению информационной безопасности медицинского учреждения, информация, подлежащая защите, а также риски и угрозы информационной системы. Приведены экономические аспекты управления информационной безопасностью. Рассмотрена возможность управления рисками и угрозами с помощью программного продукта ГРИФ.*

Общая постановка проблемы

Широкое применение информационных технологий создало проблемы не только производительности, надежности и устойчивости функционирования информационных систем, а также проблемы защиты циркулирующей в системах информации от несанкционированного доступа.

Актуальной является информационная безопасность для частных клиник, так как важна защита конфиденциальной информации согласно Закону Украины "О защите персональных данных".

Исследования

Сегодня информация является как инструментом в работе сотрудника частной клиники, так и продуктом его работы, требования к обеспечению информационной безопасности медицинского учреждения должны сводиться к трем основным пунктам:

- недопущение несанкционированного доступа к информационным ресурсам клиники;
- противодействие уничтожению, блокированию, копированию, подделке, хищению или изменению информации (как намеренному, так и случайному);
- обеспечение бесперебойности и качества функционирования информационных систем, их аппаратных модулей и программного обеспечения.

Подлежат защите следующие информационные ресурсы частной клиники:

- амбулаторные карты;
- истории болезни;
- поля базы данных медицинской, бухгалтерской и пр. информационных систем;
- личные дела и трудовые книжки сотрудников и др.

Задача сохранения врачебной тайны решается посредством разграничения полномочий доступа к информации и применением специальных программно-аппаратных средств.

Использование информационных систем связано с определенной совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

Суть мероприятий по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки.

Подвергнуться внешнему воздействию или выйти из строя могут такие компоненты информационной системы как: аппаратные средства, программное обеспечение, данные, персонал.Общая классификация угроз автоматизированной информационной системы объекта описана ниже.

1. Угрозы конфиденциальности данных и программ. Реализуются при несанкционированном доступе к данным, программам или каналам связи.

2. Угрозы целостности данных, программ, аппаратуры. Целостность данных и программ нарушается при несанкционированном уничтожении, добавлении лишних элементов и модификации записей о состоянии счетов, изменении порядка расположения данных, формировании фальсифицированных платежных документов в ответ на законные запросы, при активной ретрансляции сообщений с их задержкой. Несанкционированная модификация информации о безопасности системы может привести к несанкционированным действиям (неверной маршрутизации или утрате передаваемых данных) или искажению смысла передаваемых сообщений. Целостность аппаратуры нарушается при ее повреждении, похищении или незаконном изменении алгоритмов работы.

3. Угрозы доступности данных. Возникают в том случае, когда объект (пользователь или процесс) не получает доступа к законно выделенным ему службам или ресурсам. Эта угроза реализуется захватом ресурсов, блокированием линий связи несанкционированным объектом в результате передачи по ним своей информации или исключением необходимой системной информации. Эта угроза может привести к ненадежности или плохому качеству обслуживания в системе и, следовательно, потенциально будет влиять на достоверность и своевременность доставки платежных документов.

Информационная среда предприятия, вне зависимости от своего состава, должна предусматривать систему безопасности. Однако затраты на обеспечение высокого уровня безопасности могут оказаться неоправданно высокими. Нахождение разумного компромисса, выбор приемлемого уровня безопасности при допустимых затратах является обязательным условием постановки задачи управления рисками в информационной системе.

Существует ряд методов, способствующих оптимизации управления информационной системой. В данной работе будет рассмотрен программный продукт ГРИФ 2006 от разработчика Digitalsecurity.

ГРИФ – это комплексная система анализа и управления рисками информационной системы компании. ГРИФ 2006 (DigitalSecurityOffice) показывает защищенность информационных ресурсов в системе и позволяет выбрать оптимальную стратегию защиты корпоративной информации.

Система ГРИФ анализирует уровень защищенности ресурсов, оценивает возможный ущерб от реализации угроз ИБ и помогает управлять рисками, выбирая контрмеры.

Анализ рисков информационной системы проводится двумя способами: при помощи модели информационных потоков или модели угроз и уязвимостей, в зависимости от исходных данных и интересующих пользователя выходных данных.

Оценка риска выполняется по двум факторам: вероятность реализации ($Р_{реализации}$) и размер ущерба.

Риск = $Р_{реализации}$× Ущерб

Дальнейшая детализация вероятности реализации:

$P_{реализации} = P_{угрозы} \times P_{уязвимости}$

На этапе ввода данных и формирования общей картины предприятия заполняются поля программы ГРИФ, соответствующие рискам информационной безопасности рассматриваемой информационной системы. Результатом обработки этих данных является график, отображающий вероятность реализации угроз (рис. 1).

Результатом работы системы ГРИФявляется отчет, содержащий расчеты затрат компании на ИБ, на контрмеры, вероятности реализации рисков в общем и по отделам и другую информацию, представленную в виде обобщающих диаграмм, графиков и таблиц.Отчет предоставляется в формате *.dsrерили *.html. Наиболее важная информация из отчета системы ГРИФ, касающаяся управления информационной безопасностью клиники «Семья+», приведена далее.

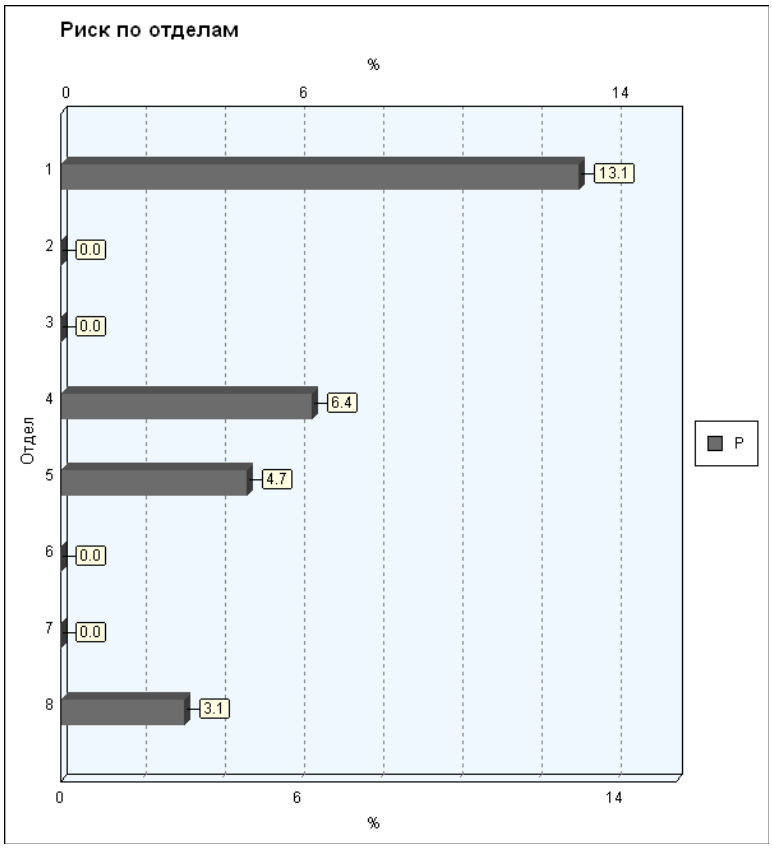

Рисунок 1 – Риск по отделам частной клиники

В таблице 1 приведена оценка уровня риска для каждого отдела клиники.

Таблица 1 – Уровень риска по отделам клиники

№	Отдел	Риск, ур.
1	Отдел семейной медицины	Низкий
2	Отдел диагностики	Низкий
3	Отдел физиотерапии	Низкий
4	Бухгалтерия	Низкий
5	Отдел статистики	Низкий
6	Регистратура	Низкий
7	Хозотдел	Низкий
8	Отдел управления	Низкий

Результат анализа ущерба и рисковинформационной системыклиники приведен в таблице 2.

Таблица 2 – Уровень ущерба и риска информационной системы

	Итого, ур.
Ущерб	Высокий
Риск	Средний

В таблице 3 приведены суммарные затраты в у.е. на информационную безопасность клиники «Семья+».

Таблица 3 – Затраты на информационную безопасность и риск частной клиники:

	Условные единицы (у.е.)	Уровни (ур.)
Затраты	8750.00	-
Риск	-	Средний

Принятые контрмеры по ресурсам (дляресурса база данных клиентов):
- повышение интереса сотрудников;
- уменьшение неумышленных действий;
- регламент создания паролей;
- эффективная защита операционной системы.

На рисунке 2приведена эффективность принятия контрмер для ресурса БД клиентов.

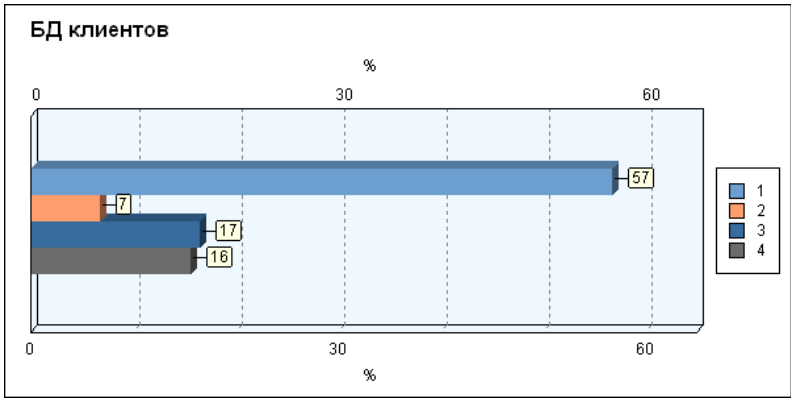

Рисунок 2 – Эффективность принятия контрмер

На таблице 4 приведены расчеты эффективности принятия контрмер для ресурса БД клиентов, а также затраты на данные контрмеры.

Таблица 4 – Эффективность принятия контрмер для БД клиентов

№	Риск до контрмеры, %	Риск после контрмеры, %	Стоимость контрмеры, ур.	Эффективность (по ресурсу), %	Эффективность (по системе), %
1	13.10	5.66	0.00	56.81	25.85
2	13.10	12.20	0.00	6.81	3.10
3	13.10	10.92	0.00	16.60	7.55
4	13.10	11.05	50.00	15.65	7.12

График, отображающий эффективность комплекса контрмер клиники, приведен на рисунке 3.

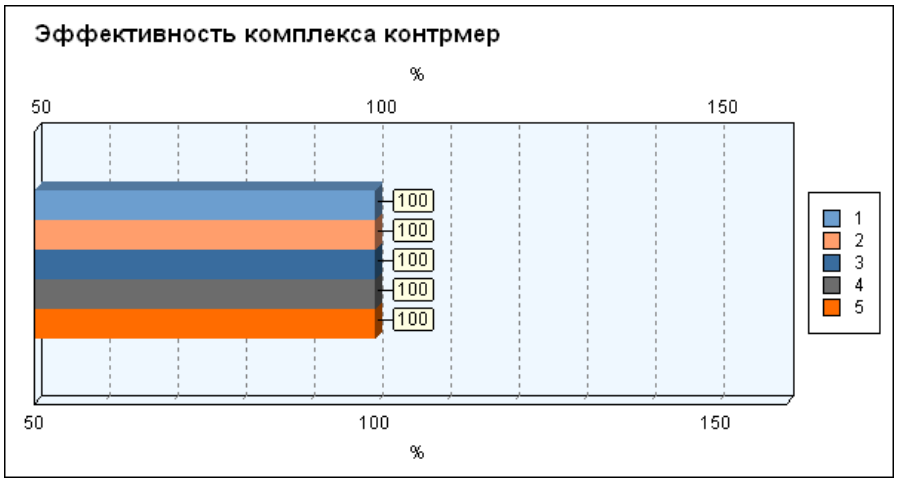

Рисунок 3 – Эффективность комплекса контрмер клиники

Таким образом, с учетом применения всех контрмер, вероятность всех рисков сводится к нулю для данной информационной системы. Это отражено в таблице 5.

Таблица 5 – Суммарная эффективность комплекса контрмер

№	Ресурс	Значение риска до всех контрмер, %	Значение риска после всех контрмер, %	Эффективность комплекса контрмер, %
1	БД клиентов	13.10	0.00	100.00
2	БД сотрудников	3.14	0.00	100.00
3	Финансовая отчетность	6.35	0.00	100.00
4	Статистическая отчетность	4.71	0.00	100.00
5	Информационная система частной клиники "Семья+"	24.88	0.00	100.00

Выводы

Решение вопросов защиты данных в современных информационных системах будет успешным только при условии использования комплексного подхода к построению системы обеспечения безопасности информации.Защищенность информации от стороннего вмешательства существенно влияет на благополучие любой организации.

В данной статье рассмотрена политика информационной безопасности для частной клиники «Семья+», с помощью программы ГРИФ проведен анализ и управление рисками клиники, в результате которого риски были сведены к нулю, а информационная система оказалась полностью защищенной.

Литература

1. ЗаконодавствоУкраїни [Electronicresourse] / Интернет-ресурс. – Режим доступа: www/ URL: http://zakon1.rada.gov.ua.– Загл. с экрана.

2. Описание программы ГРИФ 2006 [Electronicresourse] / Интернет-ресурс. – Режим доступа: www/ URL:http://www.dsec.ru.– Загл. с экрана.

3. Информационные системы: оценка рисков. А.И. Захаров [Electronicresourse] / Интернет-ресурс. – Режим доступа: www/ URL:http://www.itsecurity.groteck.ru.– Загл. с экрана.