УДК 004

Е.П. Забарина, Н.Е.Губенко
Донецкий национальный технический университет,
г. Донецк
кафедра компьютерных систем мониторинга

ПОВЫШЕНИЯ КЛАССА БЕЗОПАСНОСТИ КОМПАНИИ BINARY STUDIO

Аннотация

Забарина Е.П., Губенко Н.Е. Повышение класса безопасности компании Binary Studio. *В статье рассмотрена инфологическая структура компании и её локальная вычислительная сеть, а также модель политики безопасности. Был определён класс безопасности компании и предложены меры по его повышению.*

Ключевые слова: *информационная безопасность, политика безопасности, класс безопасности*.

Постановка проблемы. В современную, «компьютерную» эпоху проблема информационной безопасности становится весьма актуальной. Исходя из этого, были предприняты попытки по внедрению мер для повышения класса безопасности Binary Studio.

Цель статьи – разработка мер для повышения класса информационной безопасности компании Binary Studio.

Инфологическая структура и локальная вычислительная сеть компании. «Binary Studio» - международная компания с разветвлённой структурой по разработке программного обеспечения. Она предоставляет комплексные услуги для самых разных пользователей, разрабатывая и реализуя качественное программное обеспечение на Java, Delphi, C/C++ и других языках. Инфологическая структура компании, а также её локальная вычислительная сеть [1] приведены соответственно на рисунках 1 и 2 [2].

Краткое описание разработки политики безопасности. При разработке политики безопасности была использована модель [3], диаграмма которой представлена на рисунке 3. Эта модель соответствует специальным нормативным документам по обеспечению информационной безопасности, в частности – стандарту ISO/IEC 17799 «Управление информационной безопасностью» [4].

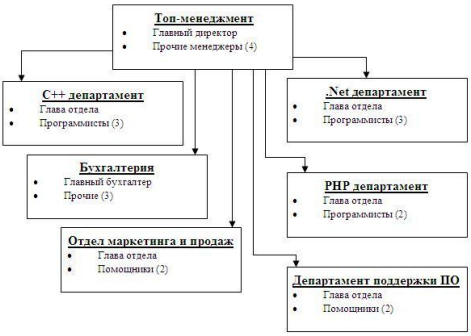

Рисунок 1 – Инфологическая структура «Binary Studio»

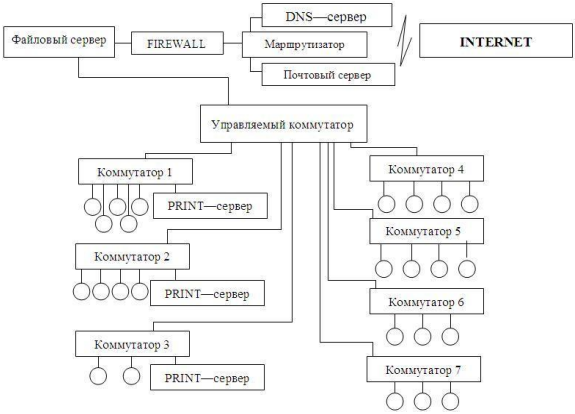

Рисунок 2 – ЛВС «Binary Studio»

Рисунок 3 – Диаграмма модели

Согласно данной модели, владелец компании стремится уменьшить риски и сохранить ресурсы за счёт использования контрмер. Нарушители создают

угрозы, которые воплощаются в уязвимости и приводят ко всяческим рискам и увеличивают потери. Поэтому политику необходимо строить из соображений защиты ресурсов во избежание возникновения рисков и угроз.

Значительное внимание в политике безопасности уделяется вопросам обеспечения безопасности информации при ее обработке в автоматизированных системах: автономно работающих компьютерах и локальных сетях. Необходимо установить, как должны быть защищены серверы, маршрутизаторы и другие устройства сети, порядок использования сменных носителей информации, их маркировки, хранения, порядок внесения изменений в программное обеспечение.

Крайне внимательно надо отнестись к подключению своих информационных ресурсов к Интернету. Идеальным с точки зрения безопасности было бы выделение для Интернета автономного компьютера без возможности хранения на нём конфиденциальной информации, с установленными антивирусными средствами защиты и правильно настроенным Firewallом. При необходимости организации распределенной работы сотрудников фирмы наиболее приемлемым решением являются виртуальные частные сети (VPN).

Несмотря на все принятые меры, нарушения информационной безопасности могут произойти. В политике безопасности должны быть обязательно предусмотрены меры ликвидации этих последствий, восстановления нормальной работоспособности фирмы, минимизации причиненного ущерба. Большое значение здесь имеет применение средств резервирования электропитания, вычислительных средств, данных, а также правильная организация документооборота [3].

Объекты и субъекты информационной защиты. Объектами информационной защиты компании Binary Studio являются все виды информационных ресурсов (исходные коды разрабатываемого программного обеспечения, бухгалтерская документация, и т.д.), система формирования и использования информации (информационные системы и технологии, архивы, нормативные документы, и т.д.), права сотрудников на получение и использование информации. Субъектами – разработчики программного обеспечения, тестировщики, сотрудники отдела поддержки, сотрудники экономического отдела.

Определение класса безопасности. Критерии определения делятся на четыре раздела: D, C, B и A, из которых наивысшей безопасностью обладает раздел A. Каждый раздел и класс расширяет или дополняет требования указанные в предшествующем разделе или классе.

На данном этапе система относится к классу безопасности C2 (Controlled Access Protection) [5].

В компании обеспечивается базовый уровень безопасности, разделяющий пользователей и данные. Соответственно, выполняются следующие основные требования:

- доверенная база управляет доступом именованных пользователей к именованным объектам;
- пользователи четко идентифицируют себя;
- аутентификационная информация пользователей защищена от несанкционированного доступа;
- доверенная вычислительная база имеет изолированную область для собственного выполнения, защищенную от внешних воздействий;
- есть в наличии аппаратные или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов доверенной вычислительной базы;
- защитные механизмы протестированы на отсутствие способов обхода или разрушения средств защиты доверенной вычислительной базы;
- описаны подход к безопасности и его применение при реализации доверенной вычислительной базы [6].

Для увеличения класса безопасности предлагается переход от дискреционного к мандатному управлению доступом к выбранным субъектам и объектам, т.е. фактически переход к классу B1 (Labeled Security Protection). После перехода к классу B1 компания будет обладать следующими характеристиками:

- доверенная вычислительная база будет управлять метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом.
- доверенная вычислительная база будет обеспечить реализацию принудительного управления доступом всех субъектов ко всем хранимым объектам.
- доверенная вычислительная база будет обеспечивать взаимную изоляцию процессов путем разделения их адресных пространств.
- группа специалистов, полностью понимающих реализацию доверенной вычислительной базы, будет подвергать описание архитектуры, исходные и объектные коды тщательному анализу и тестированию.
- будет существовать неформальная или формальная модель политики безопасности, поддерживаемой доверенной вычислительной базой [6].

Меры для повышения класса безопасности. Для того, чтобы от класса C2 перейти к классу B1, предлагается применить следующие меры:

- неформально описать модель политики безопасности;
- неформально описать модель маркировки данных;
- описание управления доступом к поименованным субъектам и объектам;
- модернизировать пирамиду доступа.

Выводы. В работе были рассмотрены следующие вопросы:

- инфологическая структура и локальная вычислительная сеть компании Binary Studio;
- основные аспекты политики безопасности компании;
- определён класс безопасности;
- предложены меры по повышению класса безопасности системы.

Предложенные меры по повышению класса безопасности могут снизить риски и угрозы предприятия. В дальнейшем возможен переход к более высокому уровню.

Список литературы

1. Offshore Custom Software Development Company|Binary Studio, Ukraine/Интернет-ресурс. – Режим доступа: www/ URL: http://www.binary-studio.com - Загл. с экрана.
2. Разработка и реализация политики безопасности предприятия/Интернет-ресурс. – Режим доступа: www/ URL: http://bezopasnik.org/article/56.htm - Загл. с экрана.
3. Международный стандарт ISO 17799 – ISO_IEC_17799_2000_RUS/Интернет-ресурс. – Режим доступа: www/ URL: http://www.kmgep.kz/data/filedat/default/ISO_IEC_17799_2000_rus.pdf - Загл. с экрана.
4. Критерии безопасности компьютерных систем/Интернет-ресурс. – Режим доступа: www/ URL: http://ru.wikipedia.org/wiki/Критерии_безопасности_компьютерных_систем - Загл. с экрана.
5. Классы информационной безопасности в международных стандартах/Интернет-ресурс. – Режим доступа: www/ URL: http://www.arinteg.ru/articles/klassy-informatsionnoy-bezopasnosti-v-mezhdunarodnykh-standartakh-30970.html - Загл. с экрана.
6. «Оранжевая книга»/Интернет-ресурс. – Режим доступа: www/ URL: http://protect.htmlweb.ru/orange1.htm - Загл. с экрана.
7. Локальная вычислительная сеть/Интернет-ресурс. – Режим доступа: www/ URL: http://ru.wikipedia.org/wiki/ЛВС - Загл. с экрана.
8. Годла А.С., Губенко Н.Е. Разработка политики информационной безопасности предприятия на основе распределенной модели использования ресурсов, – Інформаційні управляючі системи та комп'ютерний моніторинг (ІУС КМ–2013): IV Всеукраїнська науково-технічна конференція студентів, аспірантів та молодих вчених, 24-25 квітня 2013 р. – Донецьк: ДонНТУ, 2013.– в 2тт. – Т2. 444 с.; с.9-15.