XXIX Неделя науки СПбГТУ. Материалы межвузовской научной конференции. Ч.V: С.104-105, 2001.

УДК 50.41.00

А.С. Монин (6 курс), С.С. Корт, доц., к.т.н.

СБОР ИНФОРМАЦИИ ПРИ ПОСТРОЕНИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

В данном докладе описан подход к сбору информации при выполнении типового системного проекта разработки предложений по обеспечению информационной безопасности некоторого предприятия или разработке политики безопасности организации.

Под политикой безопасности понимается набор правовых, организационных и технических мер по защите информации, принятый в конкретной организации. Для того чтобы определить, от каких именно угроз и каким образом защищает информацию вычислительная система, необходимо сформулировать ее политику безопасности.

Таким образом, политика безопасности подразумевает множество условий, при которых пользователи системы могут получить доступ к информации и ресурсам. С одной стороны, политика безопасности предписывает пользователям, как правильно эксплуатировать систему, с другой - политика безопасности определяет множество механизмов безопасности, которые должны существовать в конкретной реализации вычислительной системы.

Кроме политик безопасности, направленных непосредственно на отражение угроз безопасности существуют политики безопасности, обладающие особыми характеристиками и используемые в частном секторе. Примерами данных политик являются политика “пресс-релиза” (информация считается секретной до определенной даты), ролевой контроль доступа и т.д.

На высоком уровне описание политики безопасности выглядит схожим для многих организаций, например: “ценная информация, обрабатываемая в организации, должна быть правильно защищена от преднамеренного или случайного раскрытия, изменения или задержки в предоставлении”. Но для различных организаций раскрытие данного определения может иметь совершенно разные последствия. Процесс уточнения высокоуровневой политики безопасности до политики безопасности, реализуемой непосредственно вычислительной системой, включает выбор многих решений от высокоуровневых, описывающих политику безопасности системы до выбора программно-аппаратной реализации.

Первой частью при выполнении типового системного проекта является сбор информации, включающий три стадии:

1. Оценка существующей структуры сети предприятия;
2. Оценка ценности информации, обрабатываемой в сети предприятия;
3. Оценка угроз информации и рисков.

Для оценки угроз и рисков необходимо оценить информацию, обрабатываемую в системе, а также проанализировать, какие пользователи, в соответствии с организацией работы вычислительной системы имеют доступ к соответствующим типам информации. Информация при обработке и хранении должна быть защищена от неавторизованного раскрытия и модификации. Очевидно, что создаваемая информация не является одинаковой. Классификация информации по категориям необходима для определения относительной ценности и разработки механизмов контроля, сохраняющих данную ценность для организации.

Для систематизации собранной информации целесообразно составить три таблицы. В табл. 1 должно быть определено соответствие организационных структур предприятия и подсетей вычислительной системы, которые используют соответствующие структуры.

Данная таблица должна быть дополнена рисунками, отображающими взаимосвязь подсетей предприятия.

Таблица 1. Подразделения предприятия и их подсети

N п.п.	Название	Номер подсети

В табл. 2 определены типы информации, значимость их по отношению к конфиденциальности, целостности и доступности. Также в этой таблице определены структуры, имеющие доступ к информации соответствующего типа (цифра в соответствующей графе соответствует номеру подразделения из первой таблицы), а также структуры, имеющие право модифицировать данную информацию.

Таблица 2. Информация, обрабатываемая в вычислительной системе предприятия

Информационные ресурсы	Подразделения, имеющие доступ	Тип потери	Стоимость

И, наконец, для дальнейшего построения профиля защиты и оценки рисков необходимо выявить существующие роли пользователей в вычислительной системе предприятия. При этом необходимо на этапе сбора информации описать приложения, с которыми должен работать пользователь и доступные ему системные ресурсы. Описание ролей пользователей в вычислительной системе предприятия приведено в табл. 3.

Таблица 3. Роли пользователей в вычислительной системе предприятия

Деловые функции	Пользователи	Приложения	Система	Системные ресурсы доступные удаленно (сервер + сервис)

Таким образом, в настоящем докладе описан этап сбора информации для построения политики безопасности вычислительной системы предприятия.