ЗАЩИТА ИНФОРМАЦИИ В IP-СЕТЯХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Щерба Д.С.
Астровский И.И. – к.т.н.,доцент

В наши дни информация становится одним из основных средств решения проблем и задач государства, различных коммерческих структур и отдельных людей.

С точки зрения защиты информация обладает рядом свойств:

Информация доступна человеку, если она содержится на материальном носителе. Различают носители - источники информации, носители - переносчики информации и носители - получатели информации.

Ценность информации оценивается степенью полезности ее для пользователя (собственника, владельца, получателя). Информация может обеспечивать ее пользователю определенные преимущества: приносить прибыль, уменьшить риск в его деятельности в результате принятия более обоснованных решений и т.д.

Информацию можно рассматривать как товар. Цена информации, как любого товара, складывается из себестоимости и прибыли.

Себестоимость определяется расходами владельца информации на ее получение путем:

- проведения исследований в научных лабораториях, аналитических центрах и т.д.;
- покупки информации;
- добывания информации противоправными действиями.

Прибыль от информации ввиду ее особенностей может принимать различные формы, причем денежное ее выражение является не самой распространенной формой. В общем случае прибыль от информации может быть получена в результате следующих действий:

- продажи информации на рынке;
- материализации информации в продукцию с новыми свойствами или технологии, приносящими прибыль;
- использования информации для принятия более эффективных решений.

Ценность информации изменяется во времени. Распространение информации и ее использование приводят к изменению ее ценности и цены. Характер изменения ценности во времени зависит от вида информации. Ценность большинства видов информации, циркулирующей в обществе, со временем уменьшается – информация стареет.

Невозможно объективно (без учета полезности ее для потребителя, владельца, собственника) оценить количество информации.

При копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а цена снижается. Так как при каждом копировании увеличивается число ее законных и незаконных пользователей, то в соответствии с законами рынка цена уменьшается [1].

Ввиду развития информационных технологий, на предприятиях и в государственных учреждениях большая часть информации обрабатывается с использованием средств вычислительной техники. Чтобы обеспечить оперативный обмен и обработку информации, а также повысить эффективность работы сотрудников, строятся компьютерные сети, что, в свою очередь, вызывает проблему защиты, обрабатываемой на средствах вычислительной техники и передаваемой по сети информации.

Для защиты информации следует регламентировать доступ к информационным ресурсам между сотрудниками предприятия и предотвратить несанкционированный доступ к данным как изнутри корпоративной сети, так и извне.

Защита информации — деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. К защищаемой относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации [2].

Существует две категории угроз информационной безопасности интеллектуальной собственности организации – внешние и внутренние угрозы. Данная классификация предусматривает разделение угроз по локализации злоумышленника (или преступной группы), который может действовать как удалённо, пытаясь получить доступ к конфиденциальной информации предприятия при помощи сети интернет, либо же действовать посредством доступа к внутренним ресурсам IT-инфраструктуры объекта.

В случае внешних атак, преступник ищет уязвимости в информационной структуре, которые могут дать ему доступ к хранилищам данных, ключевым узлам внутренней сети, локальным компьютерам сотрудников. В этом случае злоумышленник пользуется широким арсеналом инструментов и вредоносного программного обеспечения (вирусы, трояны, компьютерные черви) для отключения систем защиты, шпионажа, копирования, фальсификации или уничтожения данных, нанесения вреда физическим объектам собственности и т.д.

Внутренние угрозы подразумевают наличие одного или нескольких сотрудников предприятия, которые по злому умыслу или по неосторожности могут стать причиной утечки конфиденциальных данных или ценной информации. Рассмотрим эти категории рисков информационной безопасности подробнее.

Для решения проблем, связанных с защитой информации необходимо постоянно отслеживать, анализировать и синтезировать оперативные данные, касающиеся атак на информацию, стремиться выделять новые угрозы и оценивать риски, связанные с ними. Важно подбирать наиболее подходящие способы защиты информации, с целью минимизации риска потери конфиденциальной информации.

Для успешной защиты информации требуются специалисты с глубокими знаниями в этой области и опытом работы. Обучение в этой сфере требует больших затрат и вложений и т.д. Наиболее приемлемым дополнением к лекционным занятиям и изучению литературы является применение обучающих и тестирующих программ. Они позволяют моделировать различные ситуации (угрозы, потенциальные проникновения) и разрабатывать новые способы защиты.

В работе намечается сделать обучающую программу, которая облегчит обучение специалистов в сфере защиты информации.

Список использованных источников:

1. Электронный ресурс. – Режим доступа: https://studfiles.net/preview/4515436/
2. Шаньгин В.Ф.. Информационная безопасность и защита информации. М: ДМК Пресс, 2014, 702с.