Филиал государственного бюджетного образовательного учреждения высшего образования Московской области
«Международный университет природы, общества и человека «Дубна» - Дмитровский институт непрерывного образования

Кафедра гуманитарных и социально-экономических наук

Угрозы безопасности информации. Преднамеренные угрозы.

Выполнил: студент группы 1014-Л
направления «Менеджмент»
Профиль «Логистика»
Филиппов Александр.

Дмитров, 2015

ЗНАЧЕНИЕ

Угрозы безопасности информации — это некая совокупность факторов и условий, которые создают опасность в отношении защищаемой информации.
Для того чтобы определить угрозы, от которых необходимо обезопасить информацию, нужно определить объекты защиты.
Ведь информация — это некоторые данные, носителями которых могут быть как материальные, так и нематериальные объекты.

НОСИТЕЛИ ИНФОРМАЦИИ

К примеру, носителями конфиденциальной информации могут быть документы, технические средства обработки и хранения информации и даже люди.

Документационными носителями информации могут быть проекты, бизнес-планы, техническая документация, контракты и договора, а также картотеки отдела кадров (персональные данные) и отдела по работе с клиентами. Отличительной их особенностью является зафиксированность данных на материальном объекте — бумаге.

Техническими средствами обработки и хранения информации являются персональные компьютеры, ноутбуки, серверы, сканеры, принтеры, а также съемные носители (переносные жесткие диски, флеш-карты, CD-диски, дискеты) и т.п. Информация в технических средствах хранится и обрабатывается в цифровом виде. Зачастую конфиденциальные данные отправляются через Интернет, например, по электронной почте. В сети они могут быть перехвачены злоумышленниками. Кроме того при работе компьютеров из-за их технических особенностей обрабатываемые данные преобразуются в электромагнитные излучения, распространяющиеся далеко за пределы помещения, которые также могут быть перехвачены и использованы в недобросовестных целях.

Люди также могут быть «носителями» информации. Например, сотрудники компании, которые имеют или могут иметь доступ к конфиденциальной информации. Таких людей называют инсайдерами. Инсайдер необязательно является злоумышленником, но в любой момент может им стать. Кроме того несанкционированный доступ к конфиденциальной информации могут получить посетители, клиенты или партнеры, а также обслуживающий персонал.

НАРУШЕНИЕ ИНФОРМАЦИИ

Теперь, когда мы понимаем, что нужно защищать, можно перейти непосредственно к рассмотрению угроз.

Они могут заключаться как в нарушении конфиденциальности, так и в нарушении достоверности, целостности и доступности информации.

- Нарушением конфиденциальности является утечка данных, несанкционированный доступ или разглашение информации.
- Нарушение достоверности информации — это фальсификация данных или подделка документов.
- Искажение, ошибки при передаче информации, потери части данных являются нарушением целостности информации.
- А блокирование доступа к информации, выведение из строя средств связи, технических средств являются нарушением доступности.

По методам воздействия на информацию угрозы подразделяются на естественные и искусственные. В свою очередь искусственные угрозы состоят из преднамеренных и непреднамеренных.

Угрозы ИБ

Естественные

- стихийные бедствия;
- пожары;
- наводнения;
- техногенные аварии;
- и другие явления, не зависящие от человека.

Искуственные

Преднамеренные

- кража (копирование) документов;
- подслушивание переговоров;
- несанкционированный доступ к информации;
- перехват информации;
- внедрение (вербовка) инсайдеров;
- фальсификация, подделка документов;
- диверсии;
- хакерские атаки и т.п.

Непреднамеренные

- ошибки пользователей;
- неосторожность;
- невнимательность;
- любопытство и т.п.

ПРЕДНАМЕРЕННЫЕ УГРОЗЫ

Преднамеренные угрозы обычно связаны с действиями, какого либо человека, причинами которых могут выступать определенное недовольство своей жизненной ситуацией, а именно материальный интерес или простое развлечение с самоутверждением своих способностей, как у хакеров.

Преднамеренные угрозы можно разделить на:

- Пассивные угрозы – предназначены в основном на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на нормальную работу самой системы. К пассивным угрозам можно отнести несанкционированный доступ к базам данных, прослушивание каналов связи.
- Активные угрозы – имеют цель нарушения нормальной работы системы, путем целенаправленного воздействия на ее компоненты. К активным угрозам можно отнести, например, вывод из строя операционной системы компьютера, разрушение ПО компьютеров, нарушение работы линий связи и т.д.

ЗАЩИТА ИНФОРМАЦИИ

Основными целями и задачами технической защиты являются:

- - защита носителей информации от полного уничтожения в результате различных природных и техногенных воздействий;
- - предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения;
- - предотвращение утечки информации по различным техническим каналам.

Если речь идет о персональной информации отдельного пользователя ПК, то главной опасностью является потеря данных по непреднамеренным причинам, а также из-за проникновения вредоносных вирусов. Основные правила безопасности, которые следует соблюдать, такие:

- периодически осуществлять резервное копирование: файлы с наиболее важными данными дублировать и сохранять на внешних носителях;
- регулярно осуществлять антивирусную проверку компьютера;
- использовать блок бесперебойного питания.