К ВОПРОСУ О ПРОБЛЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

В. В. Христич, канд. техн. наук, доцент,
М. В. Маляров, канд. техн. наук, доцент
Национальный университет гражданской защиты Украины,
Украина, г. Харьков

Современное развитие общества характеризуется всевозрастающей ролью информационных воздействий, которые представляют собой совокупность различных информационных инфраструктур и субъектов, осуществляющих сбор, формирование, распространение и использование информации. Массовая компьютеризация, внедрение и развитие новейших информационных технологий привели к существенным изменениям в сферах образования, бизнеса, промышленного производства, научных исследований и социальной жизни. Информация превратилась в глобальный ресурс человечества [1].

Современный переход в хранении информации с бумаги на цифровые носители поставил новый и очень важный вопрос о том, как эту информацию защитить, поскольку очень большое количество различных факторов влияет на сохранность данных, в том числе и конфиденциальных.

Сегодня для организации безопасного хранения данных, первым делом проводится анализ влияющих факторов — угроз, что позволяет правильно спроектировать схему информационной безопасности.

Существует несколько основных принципиальных типов угроз информационной безопасности, которые требуют обязательного внимания – естественные и искусственные угрозы [2].

Первый тип — естественные угрозы. К ним относятся пожары, наводнения, ураганы, удары молний и другие стихийные бедствия и явления, которые не зависят от человека. Наиболее частыми среди этих угроз являются пожары. Для обеспечения безопасности информации, необходимым условием является оборудование помещений, в которых находятся элементы системы (носители цифровых данных, серверы, архивы и пр.), противопожарными датчиками, назначение ответственных за противопожарную безопасность и наличие средств пожаротушения.

Соблюдение всех этих правил даст возможность минимизировать потери информации от естественных угроз, в частности, от пожара. Если помещения с носителями ценной информации располагаются таким образом, что они подвержены угрозе наводнения, то единственное что можно предпринять в данной ситуации — это исключить хранение носителей информации на первых этажах здания, которые подвержены затоплению. Еще одной естественной угрозой являются молнии. Очень часто при ударах молнии выходят из строя сетевые карты, электрические подстанции и другие устройства. Особенно ощутимые потери, при выходе сетевого оборудования из строя, несут крупные организации и предприятия. Во избежа-

ние подобных проблем соединительные сетевые кабели экранируются, а экран кабеля заземляется. Для предотвращения ущерба от молнии устраиваются заземления, а компьютеры и серверы комплектуются источниками бесперебойного питания.

Второй тип угроз – искусственные, которые делятся на непреднамеренные и преднамеренные. Непреднамеренные угрозы — это действия, которые совершают люди по неосторожности, незнанию, невнимательности или, в частности, из-за любопытства. К такому типу угроз относят установку программных продуктов, которые не входят в список необходимых для работы персонала, а в последствии могут стать причиной нестабильной работы ПК, системы в целом, что может привести к потере информации. Сюда же можно отнести и другие действия, в частности, персонала, которые не являлись злым умыслом, а совершавшие их, не осознавали всех последствий. Этот вид угроз тяжело поддается контролю. Недостаточно, чтобы персонал был квалифицирован, необходимо чтобы каждый осознавал риск, возникающий при его несанкционированных действиях.

Преднамеренные угрозы – это угрозы, связанные со злым умыслом физического преднамеренного вывода системы из строя, и, возможно, её последующего разрушения. К преднамеренным угрозам относятся внутренние и внешние воздействия. Однако, несмотря на распространенное мнение, крупные компании несут потери зачастую не от хакерских атак, а по вине своих же сотрудников. И известно немало таких примеров.

К внешним преднамеренным угрозам можно отнести угрозы хакерских атак. В таком случае, при условии, что информационная система связана с глобальной сетью Интернет, то для предотвращения хакерских атак необходимо использовать межсетевой экран, так называемый firewall, который может быть, как встроен в оборудование, так и реализован программно.

Соблюдение всех мер предосторожности и защиты [3] от возможных потенциальных угроз, в частности, перечисленных выше, позволит достаточно надежно защитить информацию.

Библиографический список

1. Информационная безопасность и защита информации Мельников В. П. и др. / Под ред. Клейменова С. А.– М.: ИЦ «Академия», 2008.– 336 с.

2. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Щербаков А. Ю. – М.: Книжный мир, 2009.– 352 с.

3. Стандарты информационной безопасности Галатенко В. А.– М.: Интернет-университет информационных технологий, 2006. – 264 с.