УДК 338.23

ЗАЩИТА КОММЕРЧЕСКОЙ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЕЁ РОЛЬ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

***П.В. Козел**, магистрант*
*Научный руководитель – **О.В. Орешникова**, к.э.н., доцент*
Полесский государственный университет

По мере совершенствования технологий и в связи с постоянно растущими потребностями человека, всё более остро становился вопрос о методах обработки и хранения неустанно увеличивающегося объёма информации. Вместе с тем совершенствовались средства получения информации, начиная от самых простых механических изобретений и доходя до современных суперкомпьютеров, а также развиваются и сопутствующие математические теории.

Информационные технологии стали стремительно развиваться уже с начала шестидесятых годов XX века, этому поспособствовало активное развитие первых информационных систем, ещё больший рост наблюдался в 90-х годах, что было связано с развитием интернета. Информационная

система имеет много предназначений – это поиск информации, её обработка, безопасное хранение, также сюда относятся и организационные ресурсы, способствующие распространению данной информации (люди, техника, финансы и т.д.).

Постепенно мы подошли к самой сути понятия информационных технологий. Информационные технологии(ИТ) подразумевают под собой совокупность процессов, методов сбора, поиска, обработки и хранения, накопления и передачи, а также предоставления информации, различные способы осуществления таких методов и процессов. Информационные технологии призваны решать задачи по эффективной организации информационного процесса, для минимизации затрат времени, труда, энергии и материальных ресурсов в различных сферах человеческой деятельности. Всё это становиться возможным благодаря рациональному использованию современных достижений в областях компьютерной техники, средствах коммуникаций, программного обеспечения и т.д. Эффективная обработка, сортировка и выборка данных, для осуществления процессов взаимодействия пользователя и компьютера, налаживание оперативных связей, удовлетворение потребностей в получении интересующих данных и многое другое возможно только с помощью информационных технологий [1, с. 127].

Одним из главных вопросов становиться вопрос защиты информации. В связи с технологическим прогрессом также усовершенствовались пути, методы и возможности для хакерского вмешательства в различные системы и бизнес, поэтому вопрос безопасности всех видов деятельности становится всё более актуальным.

Обеспечение конфиденциальности информации (доступ к интересующей нас информации могут иметь только авторизированные пользователи, которые обладают для этого определённым уровнем доступа), обладать целостностью (считаться достоверной, содержать полноту информации, а также методы и алгоритмы её обработки) и не менее важное составляющее это доступность (обеспечить доступ авторизированным пользователям по мере необходимости) законным пользователям. В этих факторах и заключается термин безопасности информации [2, с. 126].

Суть термина безопасности информации заключается в следующем: состоянии информации, при котором она защищена от любых видов угроз; отсутствие возможности какой-либо утечки по различным каналам; гарантия того, что на данные и иные части автоматизированной информационной системы, будет оказано какое-либо несанкционированное воздействие.

Угрозы – непредумышленные воздействия или акты злоумышленников, выводящие из состояния безопасности, со стороны наружного окружения и внутренних источников. Им подвержены: персонал, имущество, информация, а также услуги и товары при их перемещении. В качестве носителей угроз безопасности выступают своего рода источники угроз. Источниками угроз являются в равной степени, как субъекты (личности), так и довольно объективные проявления (злоумышленники, соперники и прочее).

Существуют три основные группы источников угроз, которые получили свою классификацию в зависимости от рода происхождения, степени прогнозирования и скорости принятия мер по устранению их последствий.

1) Антропогенные источники. Характеризуются тем, что действия, послужившие причиной нарушения безопасности информации можно классифицировать как запланированные или случайные преступления. Однако данный тип источников возможно предугадать и достаточно быстро принять соответствующие действия по их устранению. Можно классифицировать источники по пути воздействия: внешние (вмешательство произошло извне) или внутренними (вмешательство происходило непосредственно изнутри). 2) Техногенные источники. Характеризуются тем, представленные источники возможно предсказать с меньшей степенью. Такие источники непосредственно связаны с техническими характеристиками подконтрольного оборудования и, следовательно, требуют пристального внимания от пользователя. Существует так же разделение таких угроз на внешние и внутренние. 3) Стихийные источники. Характеризуются тем, что эта группа содержит в себе условия, собирающие природные катаклизмы или иные обстоятельства, которые невозможно предусмотреть заранее или предотвратить, или же имеется возможность предусмотреть, но нет возможности предотвратить, обстоятельства, носящие непредвзятый и глубокий характер. Возможно наибольшую степень опасности представляет именно данный тип угроз, так как имеет стихийных характер и распространяется на всех. Прогнозированию представленный тип абсолютно не поддаётся и, следовательно, меры против них должны применяться всегда. Зачастую к данному типу относят различные природные катаклизмы и катастрофы, и поэтому можно считать, что приведённые источники имеют внешний относительно защищаемого объекта характер [3, с. 97].

Защита прав собственности информации, обеспечение её целостности, достоверности и сохранности, заключающаяся в защите от изменений, потери, утечки, копирования или же блокирования информации злоумышленниками, является основной целью обеспечения безопасности информации.

Для сохранения информации в безопасности и поддержания её в первозданном виде (полной и структурированной), необходимо проводить ряд мер по защите информационных ресурсов, и путей поступления информации. Безопасность информации всегда была и остается одной из ведущих частей военной безопасности и непосредственно относиться к защите ресурсов, связанных с информацией, всех знаний, каналов, методов хранения информации, её преобразования и обрабатывающих алгоритмов, которые используется не только для гражданской обороны, защищающие жизненно необходимые интересы не только отдельных граждан и общества, а всего государства в целом [4, с. 109].

Защита информации, которая непосредственно является коммерческой или государственной тайной (как совершенно любой вид информации), нужна для осуществления научной, управленческой и иных видов деятельности. Обеспечение безопасности информации в информационных системах является первостепенной задачей защиты информации. Объясняется это многими факторами, и как основную причину можно привести то, что все более широкое распространение в накоплении и обработке информации получают электронные ресурсы, которые подвержены не только утечкам информации, но и её разрушении, искажении, подделке, блокировании и иным вмешательствам в информацию и информационные системы, хотя нельзя упускать тот факт, что любого вида информация подвержена данным угрозам.

Все что было сказано выше постепенно подводит нас к общему выводу. С каждым годом технологии совершенствуются и несомненно это ведёт к заметному улучшению любых видов человеческой деятельности, и, к сожалению, хакерской тоже. Стоит также помнить и тот факт, что любая информация (коммерческая, государственная и т.п.) имеет свою ценность, и в наших интересах остаётся обеспечение её безопасности. Именно поэтому я считаю, что защита информации любого вида играет большую роль в информационных технологиях.

Список использованных источников

1. Алёшин Л.И. Тема 2. Информационные системы и технологии // Информационные технологии / Н.В. Максимов. – Литера, 2008. – с. 424

2. Применко Э.А. Алгебраические основы криптографии. №9. Изд.стереотип. М.: Книжный дом «ЛИБРОКОМ», 2014. - с. 294

3. Малюк А.А. Теория защиты информации. – М.: Горячая линия – Телеком, 2012. – с. 184

4. Исамидинов А.Н. Защита коммерческой тайны в сфере трудовых отношений. №11. М.: Книжный дом «ЛИБРОКОМ», 2014. - с. 120