- Schimbarea managementului informațional odată cu dotarea tehnică și instruirea personalului. Eliminarea cazurilor în care medicii sau profesorii care dispun de calculatoare, dar le utilizează doar pentru lucru intern, fără a se integra în fluxuri externe de informații, fără a se implica în schimb activ de informații cu pacienții/studenții.
- Repartizarea unor curatori din partea instituției care ar fi disponibili pentru colaborări on-line.

Bibliografie:

1. Bogdan Ghilic-Micu, *Guvernarea electronică*, Revista Informatică Economică, nr. 1 (21)/2002.
2. Daniela Gărăiman, *Repere privind eficientizarea administrației publice prin informatizare*, Revista de Ştiinţe Juridice.
3. Hotărârea Guvernului Republicii Moldova privind Strategia Națională de edificare a societății informaționale – Moldova electronică
4. http://www.ipp.md
5. http://egov.md
6. http://e-services.md
7. http://www.seap.usv.ro

ПРАВОВОЙ АНАЛИЗ ПОТЕНЦИАЛЬНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА И ГОСУДАРСТВА

С. ГРИЩУК-БУЧКА
Институт истории, Государства и Права АНР (Республика Молдова)

The threats in information security are extremely dangerous, as by means of a criminal encroachment information can be exposed to certain influences. This article presents the legal analysis by given problematics.

Информационная безопасность – состояние защищенности информационной среды общества от внутренних и внешних угроз, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государств [1]. Исходя из данного определения, объектом угроз информационной безопасности выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, финансовых ценностей, информационных ресурсов и т.д.), угрозы же выражаются в нарушении целостности и достоверности информации. Угроза выступает в качестве потенциально возможного или реального действия злоумышленников,

способного нанести моральный и материальный ущерб, и даже подорвать государственность, в частности, аспект «информационных войн».

Если ранее злоумышленники и киберпреступники, концентрировали свое внимание преимущественно на «сведениях и данных» физических лиц, то в последнее время все чаще объектом преступного посягательства выступают данные коммерческих компаний и правительственных учреждений. В частности:

- за весь 2010 год китайские правительственные сайты в общей сложности становились жертвами атак более 4 600 раз[2];
- 1 марта 2011 американский банк Morgan Stanley подвергся атаке хакеров, в результате которой в руках злоумышленников оказались закрытые данные, касающиеся деятельности банка и интересов его клиентов [3];
- 5 марта 2011 массированной кибератаке со стороны неизвестных хакеров подверглись Интернет-сайты аппарата президента Ли Мен Бака и 40 государственных учреждений Южной Кореи [4];

Подобные примеры шокируют. Весьма ужасающе в данном контексте звучат данные государственного Управления по киберпреступности Великобритании и компания Detica, - «киберпреступность ежегодно обходится британской экономике в 27 млрд фунтов стерлингов» [5].

Угрозы в сфере информационной безопасности чрезвычайно опасны, поскольку посредством преступного посягательства, «информация» может подвергаться определенным воздействиям:

- *ознакомлению*, противоправному деянию, не приводящему к изменению или разрушению информации, однако существенно снижающему ее ценность, в частности, ознакомление с конфиденциальной информацией
- *искажению*, случайным или преднамеренным преступным действиям, приводящим к частичному изменению содержания, определенной модификации сущности самой информации
- *разрушению,* противоправным действиям, приводящим к значительному или полному уничтожению информации и информационных ресурсов.

В конечном итоге, как отмечает В.И. Ярочкин, противоправные действия с информацией приводят к нарушению ее конфиденциальности, полноты, достоверности и доступности [6,20].

Базовая классификация потенциальных угроз информационной безопасности строится на положении «местонахождение источника потенциальной угрозы» и соответственно подразделяется на *внутренние*, (источник угрозы находится непосредственно внутри организации или государства) и *внешние* угрозы (источник угрозы расположен за пределами самого объекта преступного посягательства.). К внутренним угрозам следует отнести: неквалифицированную внутреннюю политику субъекта по организации информационных технологий и управлению безопасностью; преднамеренные и непреднамеренные действия персонала по нарушению правил безопасности; отсутствие соответствующей квалификации персонала по обеспечению деятельности и управлению объектами защиты [7]; предательство

персонала посредством разглашения или утечки информации, несанкционированного доступа; техногенные аварии и разрушения, пожары Источниками внутренних угроз могут быть: администрация организации или государства, персонал или чиновники, технические средства обеспечения производственной и трудовой деятельности.

Источниками внешних угроз чаще всего выступают: преступные группировки и формирования, недобросовестные конкуренты, отдельные лица и организации административно-управленческого аппарата. Среди внешних угроз выделяют: негативные воздействия недобросовестных конкурентов и государственных структур; несанкционированное проникновение на объект защиты [7]; несанкционированный доступ к носителям информации и каналам связи с целью хищения, искажения, уничтожения, блокирования информации без соответствующего вовлечения в преступные действия сотрудников или представителей потенциального субъекта-жертвы; преднамеренные и непреднамеренные действия поставщиков услуг по обеспечению безопасности и поставщиков технических и программных продуктов, стихийные бедствия и другие форс-мажорные обстоятельства.

На условном уровне соотношение внешних и внутренних угроз можно охарактеризовать, как отмечает В.И. Ярочкин, следующими показателями [6,22-23]:

- 82% угроз совершается собственными сотрудниками организации при их прямом или опосредованном участии;
- 17 % угроз совершается из вне – внешние угрозы;
- 1% угроз совершается случайными лицами.

Потенциальные угрозы в сфере информационной безопасности представляется возможным классифицировать и по иным основаниям:

- по объектам преступного посягательства: персонал, материальные или финансовые ценности, информация, стабильность общества, государственность.
- по ущербу: материальный или моральный,
- по характеру воздействия: активные и пассивные угрозы,
- по причинам появления – стихийные и преднамеренные,
- по вероятности возникновения – весьма вероятные, вероятные, маловероятные.

Представленный анализ позволяет сделать вывод о том, что потенциальные угрозы в информационной сфере в большинстве случаев носят преднамеренный и целенаправленный характер, выражающийся чаще всего в активном воздействии внутренних источников потенциальных угроз на объект преступного посягательства.

Литература

1. Организациооно-правовое обеспечение информационной безопасности: учеб. пособие для студ.высш.уч.зав./ А.А.Стрельцов. – М.: Издательский центр «Академия», 2008. – с.36
2. Китайские эксперты сообщили об увеличении числа хакерских атак на государственные сайты http://www.securitylab.ru/news/405062.php

3. Morgan Stanley стал жертвой серьезной утечки данных http://www.securitylab.ru/news/404944.php
4. Хакеры атаковали сайты 40 министерств Южной Кореи http://www.securitylab.ru/news/404990.php
5. Киберпреступники наносят Великобритании ежегодный ущерб 27 млрд фунтов http://www.securitylab.ru/news/404871.php
6. Ярочкин В.И.Информационная безопасность: учебник для вузов.-5-е издание. – М.: Академический проспект, 2008. – 544с.
7. Угрозы информационной безопасности http://itsecblog.ru/ugrozy-informacionnoj-bezopasnosti/

ПОЛИТИКА БЕЗОПАСНОСТИ И ЕЁ АНАЛИЗ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Денис ГАЛЕЦКУЛ,
Приднестровский Государственный Университет имени Т.Г.Шевченко

Локальная вычислительная сеть - компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт). Также существуют локальные сети, узлы которых разнесены географически на расстояния более 12 500 км (космические станции и орбитальные центры). Несмотря на такие расстояния, подобные сети всё равно относят к локальным.

Должны быть поставлены следующие цели при разработке эффективной защиты ЛВС:

- обеспечить конфиденциальность данных в ходе их хранения, обработки или при передаче по ЛВС;
- обеспечить целостность данных в ходе их хранения, обработки или при передаче по ЛВС;
- обеспечить доступность данных, хранимых в ЛВС, а также возможность их своевременной обработки и передачи
- гарантировать идентификацию отправителя и получателя сообщений.

Адекватная защита ЛВС требует соответствующей комбинации политики безопасности, организационных мер защиты, технических средств защиты, обучения и инструктажей пользователей и плана обеспечения непрерывной работы.

Многие организации используют средства ЛВС для обеспечения нужд обработки и передачи данных. ЛВС логически и физически рассредоточена по всей организации.

Службы безопасности, защищающие данные, а также средства по их обработке и передаче, также должны быть распределены по всей ЛВС. Пользователи должны быть уверены в том, что их данные и ЛВС адекватно защищены. Защита ЛВС должна быть интегрирована во всю ЛВС и должна быть важной для всех пользователей.