– выявление проблем (угроз) на каком-либо из уровней безопасности говорит о высокой вероятности наличия проблем и на соседних звеньях.

Таким образом, можно сделать вывод о существовании шести уровней безопасности корпорации:

1) уровень акционеров и владельцев;
2) высшее руководство корпорации;
3) организационная структура и система управления корпорации, система мотивации персонала и кадровой политики;
4) уровень построения технологических и бизнес-процессов;
5) финансовая и хозяйственная деятельности;
6) уровень учета, контроля и анализа организаций.

Каждый из этих уровней можно рассматривать как субъект безопасности, объект безопасности, источник угрозы и объект угрозы. В случае необеспечения безопасности на более высоком уровне все мероприятия внутри более низких звеньев становятся малоэффективными и порой бессмысленными. Полагаем, что уровни системы безопасности имеют и обратную зависимость: не будет обеспечена безопасность на низком уровне – все мероприятия по обеспечению безопасности на более высоких уровнях станут также малоэффективными. Это подтверждается результатами исследований в области развития корпораций[6].

**Примечания**

1 *Бородин И. А.* Основы психологии корпоративной безопасности. М., 2004.

2 *Гапоненко В. Ф., Беспалько А. Л., Власков А. С.* Экономическая безопасность предприятий. Подходы и принципы. М., 2007.

3 См.: Основы экономической безопасности (Государство, регион, предприятие, личность) / под ред. Е. Л. Олейникова. М., 1997. С. 138.

4 См.: *Половнев К. С.* Механизм обеспечения экономической безопасности промышленного предприятия : дис. … канд. экон. наук. Екатеринбург, 2002. С. 34.

5 См.: *Молдаванцев А. А.* Участие органов внутренних дел в обеспечении экономической безопасности предприятия : дис. … канд. экон. наук. М., 2004. С. 83.

6 См.: *Бородин И. А.* Указ. соч. ; *Половнев К. С.* Указ. соч. и др.

УДК 316:341.3

# СПЕЦИФИКА АКТУАЛЬНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ ОБЩЕСТВЕ

**А. Д. Хлебожаров**

Саратовский государственный университет
E-mail: AlexDKh@yandex.ru

В статье рассматриваются результаты исследований актуальных угроз информационной безопасности среди граждан и проблема информационной безопасности.
**Ключевые слова**: информационная безопасность, угрозы, социальный статус, информация.

**Specifics of Actual Threats of Information Security in Modern Society**

**A. D. Khlebozharov**

In article results of researches of actual threats of information security among people and a problem of information security are considered.
**Key word:** information security, threats, social status, information.

Современный этап общемирового развития характеризуется возрастающей ролью информационной сферы. Превращаясь в системообразующий фактор жизни общества, она все более активно влияет на состояние политической, экономической, оборонной, личной, имущественной и других составляющих безопасности.

Широкое распространение некоторых информационных технологий сопровождается появлением ряда новых угроз конституционным правам и свободам граждан, формированию здоровья, полноценной духовной жизни. Эти технологии уже используются для целей экономики, торговли, рекламы, политической борьбы, оказывая порой разрушительное воздействие на психику людей, в особенности подростков.

Информационное воздействие становится главным рычагом управления людьми, все больше заменяя физическое воздействие, тысячелетиями считавшееся непременным средством управления. Вот почему одним из основных элементов национальной, общественной и личной безопасности становится информационная безопасность, которая в современном мире выступает жизненно необходимым условием обеспечения интересов человека, общества и государства[1].

Оценка информационной безопасности является одной из наиболее актуальных в проблематике обеспечения информационной безопасности России. Это обусловлено, с одной стороны, значительными усилиями, предпринимаемыми субъектами Российской Федерации в этой области, а также существенными объемами привлекаемых

для этого финансовых и иных ресурсов, с другой – практическим отсутствием исследований эффективности этих усилий. Необходимо отметить, что и за рубежом подобные исследования начали проводить сравнительно недавно.

Угрозы информационной безопасности граждан представляют собой совокупность факторов и условий, способных оказать негативное влияние на реализацию гражданами своих интересов, связанных с имеющейся у них информацией, принадлежащими им информационными ресурсами и с использованием для обработки информации средств вычислительной техники.

В качестве основных угроз информационной безопасности граждан в данном случае целесообразно рассматривать те, с проявлениями которых граждане сталкиваются наиболее часто. Частота проявлений угроз может быть оценена долей респондентов, которые сталкивались с проявлением этих угроз в течение некоторого интервала времени, например, в течение года.

Результаты проведенного опроса позволят оценить:

– наиболее часто совершаемые информационные преступления;

– основные угрозы информационной безопасности;

Результаты социологического исследования[2] актуальных угроз информационной безопасности, с которыми сталкивались граждане за последний год, в разбивке по возрастной категории представлены в табл. 1.

*Таблица 1*

**Влияние возраста на субъективность актуальных угроз информационной безопасности, %**

| Актуальные угрозы информационной безопасности за последний год | Возраст | | | | | По выборке |
|---|---|---|---|---|---|---|
| | 15–20 | 21–25 | 26–35 | 36–45 | 46 и выше | |
| Зловредные вирусы | 33,2 | 44,0 | 52,3 | 41,5 | 45,0 | 43,2 |
| Атаки хакеров | 7,8 | 3,2 | 8,8 | 3,5 | 8,1 | 6,3 |
| Интернет-мошенничество | 33,9 | 24,5 | 18,0 | 16,7 | 15,6 | 21,8 |
| Безграмотность самих пользователей | 23,6 | 28,4 | 20,9 | 38,3 | 31,3 | 28,2 |
| Затрудняюсь ответить | 1,5 | 0,0 | 0,0 | 0,0 | 0,0 | 0,5 |
| Итого | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 |

Анализ показывает, что среди 15–20-летних пользователей самой распространенной угрозой безопасности является интернет-мошенничество (33,9% опрошенных указали на это). На втором месте – компьютерные вирусы (33,2%), на третьем месте – безграмотность самих пользователей (23,6%). Среди 21–25-летних пользователей самой распространенной угрозой безопасности являются зловредные вирусы (44%), на втором месте – безграмотность самих пользователей (28,4), на третьем месте – интернет-мошенничество (24,5%). Пользователи 26–35 лет также на первое место поставили вирусы (52,3%), на второе – собственную безграмотность (20,9%), на третье – интернет-мошенничество (18%). Так же распределились места 36–45-летних пользователей – 41,5, 38,3 и 16,7% соответственно. Среди пользователей 46 лет и старше самой распространенной угрозой безопасности являются компьютерные вирусы (45%), за ними следуют безграмотность самих пользователей (31,3%) и интернет-мошенничество (15,6%).

Как следует из результатов опроса, к числу основных актуальных угроз информационной безопасности граждан относятся:

– зловредные вирусы;

– безграмотность самих пользователей;

– интернет-мошенничество.

Если рассматривать показатель «зловредные вирусы», то одинаково большой процент показывают все возрастные категории, это связано с тем, что компьютеры используются в нашей жизни повсеместно. А это свидетельствует о том, что практически любой человек может быть подвержен атакам вирусов.

Интернет-мошенничество считает актуальной угрозой категория 15–20-летних – это связано, прежде всего, с тем, что молодежь сейчас активно использует интернет-магазины и оплату услуг через Интернет. В будущем эта категория будет только увеличиваться, и тем самым защита при работе в Интернете очень актуальна уже в данный момент.

«Атаки хакеров» показали небольшой процент среди общего числа опрошенных, это обусловлено скорее всего тем, что такие атаки осуществляются зачастую не на конкретных пользователей, а на компании, государственные учреждения. Также не исключен процент атак хакеров на личные компьютеры граждан, но это бывает очень сложно заметить, и обычные пользователи о них часто даже не догадываются.

Угроза распространения вирусов проявляется в виде противоправного размещения на средствах вычислительной техники граждан вредоносных программ. Под воздействием этих программ может быть нарушено нормальное функционирование программного и технического обеспечения вычислительной техники граждан, уничтожены или модифицированы принадлежащие им информационные ресурсы, получен противоправный доступ к информации о частной жизни, личной

и семейной тайне, к другой хранящейся и обрабатываемой конфиденциальной информации. Социальная опасность данной угрозы заключается в возможности нанесения материального или морального ущерба гражданам, размеры которого могут быть весьма значительными и зависят от степени использования потерпевшими вычислительной техники в различных областях их деятельности.

Угроза распространения незапрашиваемых рекламных сообщений (спама) проявляется в виде поступления в электронные почтовые ящики пользователей определенного (иногда значительного) количества обращений, не представляющих для граждан никакой практической ценности. Вследствие этого несколько увеличивается время, необходимое для подготовки вычислительной техники к работе, а также возникает необходимость осуществления утомительных процедур чистки электронных почтовых ящиков. Социальная опасность данной угрозы невелика, поскольку выражается, как правило, в незначительном материальном ущербе.

Угроза несанкционированного доступа к компьютеру проявляется в виде модификации или уничтожения программных средств, расположенных на данном компьютере, копирования, модификации, нарушения целостности или уничтожения хранящихся в нем информационных ресурсов, а также использования технических средств компьютера для размещения программных средств нарушителя, осуществления обработки информации в его интересах, нарушения работоспособности компьютера. Социальная опасность данной угрозы заключается в возможности нарушения установленного собственником режима информационных ресурсов, противоправного раскрытия сведений, составляющих личную и семейную тайны, либо сведений о частной жизни гражданина, воспрепятствования использованию компьютера для осуществления информационной деятельности.

Результаты социологического исследования актуальных угроз информационной безопасности, с которыми сталкивались граждане за последний год, по социальному статусу представлены в табл. 2.

*Таблица 2*

**Влияние социального статуса на субъективность актуальных угроз информационной безопасности, %**

| Актуальные угрозы информационной безопасности за последний год | Социальный статус | | | | | | | Итого |
|---|---|---|---|---|---|---|---|---|
| | Школьник | Студент | Работаю | Пенсионер | Аспирант, работаю, | Студент, работаю | Пенсионер, работаю | |
| Зловредные вирусы | 50,0 | 30,4 | 48,7 | 0,0 | 0,0 | 60,0 | 59,1 | 31,7 |
| Атаки хакеров | 50,0 | 7,4 | 6,7 | 0,0 | 0,0 | 0,0 | 4,5 | 6,8 |
| Интернет-мошенничество | 0,0 | 37,4 | 17,6 | 0,0 | 0,0 | 20,0 | 9,1 | 25,0 |
| Безграмотность самих пользователей | 0,0 | 23,3 | 27,0 | 0,0 | 100,0 | 20,0 | 27,3 | 36,0 |
| Затрудняюсь ответить | 0,0 | 1,5 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,5 |
| Итого | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 |

Анализ показывает, что среди школьников самой распространенной угрозой безопасности являются зловредные вирусы (50% опрошенных), на втором месте – атаки хакеров (50%). Среди студентов на первом месте среди угроз безопасности находится интернет-мошенничество (37,4%), на втором – вирусы (30,4%), на третьем – безграмотность самих пользователей (23,3%). Среди работающих первое место занимают вирусы (48,7%), далее идут безграмотность самих пользователей (27,3%) и интернет-мошенничество (17,6%).

Исходя из этого, можно сделать вывод, что наибольший процент показывают те граждане, которые работают, следовательно, вирусам подвергаются их рабочие компьютеры. А это, в свою очередь, говорит, что при заражении вирусом хотя бы одного компьютера может произойти заражение всех остальных и, как следствие, остановка рабочих процессов на предприятии. Данный факт свидетельствует, что на рабочих местах часто не уделяется должного внимания антивирусной политике.

Безграмотность самих пользователей отмечает большинство по каждому социальному статусу. Как правило, пользователи не знают, что делать при той или иной атаке их компьютера, тем самым упрощая, а иногда и помогая этим атакам, сами не зная того. Это указывает на то, что проблемы информационной безопасности недостаточно освещаются в обществе, в университетах, в организациях. Это приводит к тому, что люди просто не знают, с чем они сталкиваются и как с этим бороться, что, в свою очередь, очень упрощает атаки на их компьютера и данные.

Интернет-мошенничество оказалось на первом месте у студентов и работающих студентов. Это связано с тем, что они наиболее активные пользователи Интернета, интернет-магазинов.

Из результатов этих двух опросов можно сделать вывод, что актуальными угрозами информационной безопасности считаются вирусы, безграмотность самих пользователей, интернет-мошенничество.

Таким образом, главным в решении данной проблемы становится обучение населения информационной безопасности, чтобы граждане знали и могли предпринять первые действия при атаках на их компьютеры, повышать уровень безопасности работы в Интернете и проводить противовирусные политики на компьютерах предприятий и личных компьютерах. Остальные угрозы показали меньший процент, но это не значит, что этих угроз мало. Например, атаки хакеров более специализированы, и они часто атакуют сайты, сети компаний и государственные объекты с целью завладеть конфиденциальными данными.

Эти угрозы со временем будут только расти в связи с увеличением соблазнов хакерских группировок получать большие деньги путем наименьшего сопротивления, когда люди часто сами им помогают и просто невнимательны при пользовании компьютером и сохранности личных данных.

**Примечания**

[1] См.: *Петров В. П., Петров С. В.* Информационная безопасность человека и общества : учеб. пособие. М., 2007.

[2] Исследование «Информационная безопасность в обществе» было проведено нами в декабре 2011 г. методом анкетирования по выборке n = 200 человек.