



УДК 316.772.4

## СОЦИАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧЕРЕЗ ПРИЗМУ ОБЩЕСТВЕННОГО МНЕНИЯ САРАТОВЦЕВ

А. Д. Хлебозаров

Саратовский государственный университет  
E-mail: xab\_magistr@front.ru

В статье по результатам социологического исследования раскрывается отношение саратовцев к информационной безопасности, выявляется низкий уровень информационной культуры, уточняются проблемы и социальные факторы повышения эффективности защиты информационной безопасности персональных и коллективных компьютерных пользователей.

**Ключевые слова:** информационная безопасность, компьютерная защита, социологический опрос, компьютерные пользователи.

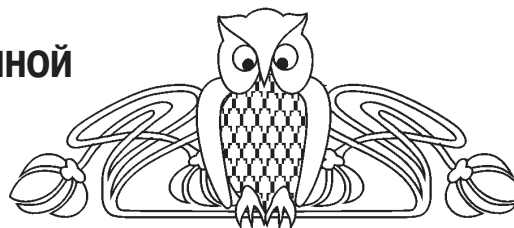
### Social Problems of Information Security Through the Prism of Saratov Inhabitants' Public Opinion

A. D. Khlebozharov

The paper summarizes the results of our sociological survey and reveals Saratov inhabitants' attitude to information security, a low level of information culture is disclosed, problems and social factors of increasing the efficiency of information security of personal and collective computer users are specified.

**Key words:** information security, computer protection, sociological poll, computer users.

В новом тысячелетии глобальное, всепроникающее и всеобъемлющее противоречие «культура безопасности человека» обозначилось как источник динамики всемирной, абсолютной безопасности, как источник мировой динамики гуманитарных перемен. Это стало главным интеллектуальным, энергетическим, мотивационным и силовым фактором возникновения, оформления и развёртывания новой глобальной структурной гуманитарной революции XXI века<sup>1</sup>. Информационная безопасность – защита конфиденциальности, целостности и доступности информации. В современном обществе – это одна из самых больших проблем как для организаций, так и конкретных пользователей. Однако часто ей не уделяется должного внимания. Более того, зачастую многие пренебрегают простейшими рекомендациями по безопасности, хотя в организациях для защиты корпоративной информации выделяются немалые материальные средства и человеческие ресурсы. И если кража корпоративной информации может привести к потере прибыли или разработки, то подделка или утечка личной переписки может привести к разрушению вполне счастливой семьи или распаду дружного коллектива. Если рассматривать информационную безопасность в том виде, в котором этим понятием



оперируем мы сейчас, то речь, конечно же, идет об информации, хранящейся или передающейся с помощью современных технических средств, высоких технологий, с помощью компьютеров.

Как следует из результатов опроса<sup>2</sup>, к числу основных актуальных угроз информационной безопасности граждан относятся вирусы (43%), безграмотность пользователей (28%), интернет-мошенничество (22%). Угроза распространения вирусов проявляется в виде противоправного размещения на средствах вычислительной техники граждан вредоносных программ. Под воздействием этих программ могут 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.

Атаки хакеров вызвали наименьшее беспокойство среди населения, так как такие атаки осуществляются зачастую не на конкретных пользователей, а на компании, государственные учреждения. Также не исключен процент атак хакеров на личные компьютеры граждан, но такие атаки бывает очень сложно заметить и о них часто даже не догадываются обычные пользователи. Между тем 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, воспре-



пятствования использованию компьютера для осуществления информационной деятельности.

Разные возрастные категории пользователей испытывают беспокойство по различным поводам. Так, среди 15–20-летних пользователей самой распространенной угрозой безопасности является интернет-мошенничество (33,9% опрошенных), на втором месте – вирусы (33,2%), на третьем – безграмотность самих пользователей (23,6%). Среди 21–25-летних пользователей самой распространенной угрозой безопасности являются зловредные вирусы (44,0%), на втором месте – безграмотность самих пользователей (28,4), на третьем – интернет-мошенничество (24,5%). Среди 26–35-летних пользователей самой распространенной угрозой безопасности являются зловредные вирусы (52,3%), на втором месте – безграмотность самих пользователей (20,9%), на третьем – интернет-мошенничество (18%). Среди 36–45-летних пользователей самой распространенной угрозой безопасности являются зловредные вирусы (41,5%), на втором месте – безграмотность самих пользователей (38,3%), на третьем – интернет-мошенничество (16,7%). Среди пользователей 46 лет и старше самой распространенной угрозой безопасности являются зловредные вирусы (45,0%), на втором месте – безграмотность самих пользователей (31,3%), на третьем – интернет-мошенничество (15,6%). Иными словами, 15–20-летние чаще других волнуют проблемы интернет-мошенничества и атаки хакеров, 21–25-летние – проблемы вирусов и интернет-мошенничества, 26–35-летние – проблемы вирусов и атаки хакеров, 36–45-летние – проблемы безграмотности пользователей. Тех, кому более 46 лет, чаще других волнуют проблемы вирусов, безграмотности пользователей и атаки хакеров. При этом по мере увеличения возраста проблема вирусов растет и достигает максимума в категории 26–35 летних, после чего актуальность этой проблемы спадает. Вероятно, это связано со снижением доли интернет-контактов и увеличением опыта пользователей. Также с возрастом растет значимость проблемы безграмотности пользователей, но снижается актуальность проблемы интернет-мошенничества. Возможно, последнее связано с тем, что именно молодежь активнее использует интернет-магазины и оплату услуг через Интернет, и можно прогнозировать, что в будущем эта категория будет увеличиваться, а актуальность проблемы возрастёт.

Исследование показало, что род деятельности и социальный статус также влияют на конкретные виды беспокойства по поводу информационной безопасности. Так, среди школьников самое большое беспокойство вызывают вирусы (50,0%) и атаки хакеров (50,0%). Среди студентов самой распространенной угрозой безопасности считается интернет-мошенничество (37,4%), затем – вирусы (30,4%) и безграмотность самих пользователей (23,3%). Работающие пользователи

на первое место ставят вирусы (48,7%), на второе – безграмотность самих пользователей (27,3%), на третье – интернет-мошенничество (17,6%). Тех, кто учится и работает, волнует только безграмотность пользователей (100%). Пенсионеры в качестве основ угрозы называют вирусы (59,0%).

Вирусы представляют собой важную социальную угрозу информационной безопасности в силу того, что им часто подвергаются рабочие компьютеры. Но при заражении вирусом хотя бы одного компьютера может произойти заражение всех остальных и, как следствие, остановка рабочих процессов на предприятии. Можно предположить, что на рабочих местах часто не уделяется должного внимания антивирусной защите.

Компьютерная безграмотность волнует самих пользователей не случайно, так как большинство из них не знает, что делать при той или иной атаке на их компьютер, тем самым упрощая, а иногда бессознательно помогая этим атакам. 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 компьютеры и данные. Таким образом, надо решать проблему обучения населения информационной безопасности, чтобы граждане знали и могли предпринять первые действия при атаках на их компьютеры, повышать уровень безопасности работы в Интернете и проводить более активную противовирусную политику как на уровне предприятий, организаций, так и на уровне личных компьютеров.

Важно уточнить, на кого общественное мнение возлагает ответственность за защиту персональных компьютеров. Выяснилось, что большинство населения (59,4%) считает ответственным за это себя. Это может говорить лишь о том, что пользователи не в полной мере оценивают масштаб информационной проблемы в современное время. Защита информации невозможна без применения специализированных знаний, методов, продуктов в области информационной безопасности.

Однако с возрастом проявляется склонность к перекладыванию этой ответственности на государство. Если в среднем так полагают 11,8%, то среди пользователей старше 46 лет так считают 28,6%, то есть в 2,5 раза больше. 26,3% опрошенных ответственность за защиту своего компьютера возлагают на специализированные фирмы, особенно на этом настаивают 15–25-летние пользователи (до 38%), 64,2% населения со средним и 35,0% – со средним специальным образованием. Саратовцы с высшим образованием (56,0%) и неполным высшим (69,2%) считают, что они справятся сами. Обладающие ученой степенью и высшей ученой степенью 100% доверяют себе в защите своих персональных данных. При



этом школьники целиком полагаются на специализированные фирмы, студенты, аспиранты, в том числе – совмещающие учебу с работой больше полагаются на себя, а каждый второй пенсионер – на государство и немного – на своих детей (12,5%).

Иными словами, патерналистские ориентации на государство сохраняются лишь в старших возрастных категориях населения и имеют тенденцию к снижению. На первый план выходит тенденция самозащиты или помощи профессионалов в обеспечении информационной безопасности граждан. Хотя для достижения информационной безопасности должны использоваться общие единые методы. Если каждый будет защищать свои данные по-своему и с учетом, что большинство пользователей у нас не владеет нужными знаниями в информационной безопасности, то в конце концов это приведет к разнообразным атакам вирусов, повреждениям персональных данных, кражи денег со счетов. Только целенаправленная и единая деятельность по осуществлению информационной безопасности может привести к эффективным результатам.

Вместе с тем выяснилось, что большинство населения (59,2%) не готово тратить средства на обеспечение своей информационной безопасности. Менее трети пользователей (27,8%) готовы тратить на это до 1000 рублей в год, еще меньше (8,0%) – до 3000 рублей. С повышением дохода населения уменьшается доля тех, кто не готов к расходам на обеспечение собственной информационной безопасности, и увеличивается доля тех, кто готов тратить на это более или менее значительные суммы денег. Даже среди самой состоятельной категории саратовцев, чей доход выше 50000 в месяц, каждый второй готов тратить на это не более 1000 рублей в год и столько же не готовы тратить вообще. Из этого можно сделать два вывода. Во-первых, многие пользователи не до конца осознают проблемы информационной безопасности и необходимость защиты своих компьютеров. Следовательно, это может спровоцировать в дальнейшем увеличение преступлений в сфере высоких технологий. Проблема информационной безопасности требует большего освещения с целью повышения грамотности населения в данном контексте. Во-вторых, то, что подавляющее большинство опрошенных считает, что они сами могут обеспечить свою информационную безопасность и не готовы тратить на это, свидетельствует об ограниченности их материальных ресурсов. Для них пользование бесплатными средствами защиты является вынужденной мерой. Это также в перспективе может способствовать росту преступлений в сфере высоких технологий.

Как следует из результатов опроса, уже сейчас 69,2% опрошенных постоянно сталкиваются с атаками вирусов, что частично приводило к потере данных, 11,5% постоянно сталкиваются с этим,

что приводит к краже конфиденциальной информации. Граждане, которые сталкиваются с атаками вирусов несколько раз в месяц и несколько раз в год, теряют свои данные в 65,0% и 61,4% соответственно. 20,0% опрошенных подвергались атакам несколько раз в месяц и 24,1% несколько раз в год, однако эти атаки ни к чему не приводили. Те, кто постоянно сталкиваются с атаками вирусов, используют бесплатные программы (66,7%) или не используют ничего (22,2%). А те, кто покупает и использует самые актуальные разработки в сфере обеспечения информационной безопасности, подвергаются атакам лишь в 11,1% случаев. Это указывает на то, что бесплатные программы не могут обеспечить информационной безопасности граждан. Можно сделать выводы, что атакам вирусов постоянно подвергается большинство компьютеров населения, особенно те, где используются малоэффективные бесплатные программы. Иными словами, затраты на информационную безопасность актуальны, и те люди, которые это понимают, меньше подвержены угрозам вирусов и других атак в сфере информационных технологий.

Из полученных результатов можно сделать вывод, что больше половины опрошенных считают информационную безопасность глобальной задачей XXI в. В настоящий момент остро стоит проблема защиты персональных компьютеров, однако она не всегда осознается пользователями. Расчет последних на самозащиту и бесплатные программы носит отчаянный вынужденный характер, когда дефицит материальных ресурсов не позволяет тратить на программы по информационной защите. С другой стороны, выявлен низкий уровень просвещенности пользователей компьютеров о необходимости и мерах по профессиональной информационной защите, пренебрежение ею (даже среди состоятельных саратовцев), что провоцирует рост преступлений в области высоких технологий и наносит значительный ущерб пользователям. Это вызывает необходимость активизации просветительской работы среди широких слоев населения о потенциальных и реальных угрозах информационной безопасности и степени эффективности бесплатных и профессиональных технологий защиты компьютерной информации.

#### Примечание

- <sup>1</sup> См.: Кузнецов В. Н. Гуманитарные взаимодействия. Социологическое исследование становления геокультурной теории безопасности : в 3 т. Т. II. Социология справедливости. Смысл мечты России – реальное достоинство каждого человека и укрощение несправедливости здесь и сейчас. М., 2008.
- <sup>2</sup> Исследование «Информационная безопасность в саратовском сообществе» было проведено в 2011–2012 гг. методом анкетирования по выборке N = 200 человек. Критерии отбора – возраст, пользование компьютером, Интернетом.