УДК 004.353 + 159.9 + 340.6

ОСОБЕННОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНАХ СУДЕБНО-МЕДИЦИНСКОЙ ЭКСПЕРТИЗЫ

Л.В. Астахова, Я.А. Сапожников

Выявлены особенности защиты персональных данных в органах судебно-медицинской экспертизы. Особенности обусловлены угрозами негативных информационно-психологических воздействий на экспертов в ходе осуществления ими профессиональной деятельности. Разработаны организационные меры по решению проблемы обеспечения информационно-психологической безопасности сотрудников органов судебно-медицинской экспертизы и перспективы их внедрения в практику защиты информации.

Ключевые слова: персональные данные, защита информации, информационно-психологическая безопасность, негативные информационно-психологические воздействия, манипуляция, судебно-медицинская экспертиза.

Введение

Недооценка проблемы обеспечения защиты персональных данных ставит под угрозу реализацию конституционных прав на свободу и личную неприкосновенность, достоинство личности, неприкосновенность частной жизни, личную и семейную тайну, а также иных прав и свобод человека и гражданина. В органах судебно-медицинской экспертизы эта проблема имеет особенности, связанные с угрозами сотрудникам этих органов со стороны информационной среды.

Для успешной судебно-экспертной деятельности необходима качественная информационная среда, под которой мы понимаем «качество потребляемой информации, защищённость субъектов от негативных информационных воздействий (информационно-психологическая безопасность) и защищённость их информации (безопасность информации), обеспечивающее полное удовлетворение информационных потребностей субъектов» [2]. Информационно-психологическая безопасность – это состояние субъекта информационного взаимодействия, при котором он защищен от негативных информационно-психологических воздействий, а также безопасно преобразует информационную среду» [3]. Под «негативными информационно-психологическими воздействиями» будем понимать «манипулятивные воздействия, которые могут осуществляться государством (в том числе иностранными), органами власти и управления и другими государственными структурами; различными общественными, экономическими, политическими организациями, в том числе зарубежными; различными социальными группами и отдельными личностями при помощи знаково-символических и образных средств, соответствующих основным модальностям органов чувств и ощущений человека, через средства массовой информации, литературу, искусство, образование, воспитание, личное общение, применение которых приводит к искажению информационно-ориентировочной основы жизнедеятельности, снижению психологического потенциала личности и другим негативным последствиям» [1].

Озабоченность государства проблемой обеспечения информационно-психологической безопасности нашла свое отражение во многих документах: «Доктрине информационной безопасности Российской Федерации» (2000), «Стратегии развития информационного общества в Российской Федерации» (2008), «Стратегии национальной безопасности Российской Федерации до 2020 года» (2009), Федеральном законе «О защите детей от информации, причиняющей вред их здоровью и развитию» (2010) и др. В начале 2000-х был также разработан проект Федерального закона «Об информационно-психологической безопасности». В проекте понятие «информационно-психологическая безопасность» определено как состояние защищенности отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере. К сожалению, проект закона был снят с рассмотрения Государственной Думой, поэтому следует заключить, что специальных, конкретных нормативных правовых решений обозначенной проблемы в России нет.

Однако нельзя сказать, что государство обошло вниманием вопросы информационных воздействий на экспертов судебной экспертизы. Согласно Федеральному Закону «О государственной судебно-экспертной деятельности в Российской Федерации» (2001 год), деятельность любого органа судебно-медицинской экспертизы основывается «на принципах законности, соблюдения прав и свобод человека и гражданина, прав юридического лица, а также независимости эксперта, объективности, всесторонности и полноты исследований, проводимых с использованием современных достижений науки и техники» [6]. Анализ нормативной базы показал, что требование о независимости эксперта дано в статье 7 названного Федерального закона: «При производстве судебной экспертизы эксперт независим, он не может находиться в какой-либо зависимости от органа или лица, назначивших судебную экспертизу, сторон и других лиц, заинтересованных в исходе дела. Эксперт дает заключение, основываясь на результатах проведенных исследований в соответствии со своими специальными знаниями. Не допускается воздействие на эксперта со стороны судов, судей, органов дознания, лиц, производящих дознание, следователей и прокуроров, а также иных государственных органов, организаций, объединений и отдельных лиц в целях получения заключения в пользу кого-либо из участников процесса или в интересах других лиц» [6]. Однако механизмы, которые могли бы качественно обеспечить выполнение этого требования, на законодательном уровне не определены.

В Федеральном законе «О персональных данных» также не определены конкретные требования к обеспечению защиты сотрудников организации от информационно-психологических воздействий. Не разработаны и типовые отраслевые решения в области защиты персональных данных, в которых могли бы быть учтены выявленные особенности.

Как показал анализ практики, выявленное противоречие становится причиной того, что в органах судебно-медицинской экспертизы выполнение статьи 7 обеспечивается в основном путем запрета пребывания в экспертных лабораториях заинтересованных в исходе дела лиц. Что касается организации обеспечения информационно-психологической безопасности, то она если и есть, то носит неформализованный характер и не встраивается ни в общую систему информационной безопасности, ни в систему защиты персональных данных органов судебно-медицинской экспертизы. Это приводит к уязвимости судебно-медицинских экспертов, увеличивая опасность негативных информационно-психологических воздействий на них.

Пути решения проблемы

Рассматривая процесс обеспечения информационно-психологической безопасности в органах судебно-медицинской экспертизы с точки зрения деятельностной методологии, мы имеем возможность определить цель, объект, субъект, процессы, средства и результаты обеспечения информационно-психологической безопасности экспертов.

Целью и результатом деятельности по обеспечению информационно-психологической безопасности в органах судебно-медицинской экспертизы является состояние защищенности информационного пространства органов судебно-медицинской экспертизы (сотрудники, технические средства, системы обеспечения функционирования технических средств, технологические процессы). Процессами деятельности по обеспечению информационно-психологической безопасности в органах судебно-медицинской экспертизы являются: 1) обеспечение защиты сотрудников от негативных информационно-психологических воздействий; 2) обеспечение недопущения негативных информационно-психологических воздействий со стороны сотрудников. Объектом выступает информационное пространство органа судебно-медицинской экспертизы. Субъектом является специалист по защите информации (совместно с кадровой службой и службой безопасности), организующий в экспертных органах обеспечение информационной безопасности, в частности – защиты персональных данных. Средствами обеспечения информационно-психологической безопасности служащих органов судебной экспертизы являются, в основном, организационно-правовые средства.

Первый шаг – информировать каждого сотрудника о том, что существуют злоумышленники, которые могут манипулировать ими. Служащие должны знать, какая информация нуждается в защите, и как эту защиту осуществлять. Однажды поняв, как можно поддаться манипуляциям извне, они будут находиться в намного более выгодной позиции, чтобы распознать атаку. Для

этого необходимо провести обучение каждого сотрудника политике и процедурам по защите информации – это необходимые и обязательные правила, которые описывают поведение сотрудников для защиты информационной системы и информации. Кроме этого, необходимо убедиться, что все понимают причину принятия того или иного положения этих правил, а потому не попытаются обойти эти правила ради материальной выгоды. Кроме того, незнанием всегда может воспользоваться злоумышленник.

Главная цель обучающей программы состоит в том, чтобы заставить сотрудников сменить их отношение к информационной безопасности, мотивировать их желание защитить информацию ограниченного доступа органа судебно-медицинской экспертизы. Основным направлением, которого следует придерживаться при разработке программы, является фокусировка на мысли, что служащие могут подвергнуться информационно-психологическому нападению в любое время. Цель органа судебно-медицинской экспертизы может считаться достигнутой, если его сотрудники будут иметь убеждение в том, что: защита информации – часть их работы; атаки злоумышленников реальны; разглашение, модификация или потеря информации может угрожать не только органу, но персонально каждому из них, их работе и благосостоянию, а также могут быть нарушены права и свободы человека и гражданина.

Второй шаг – разработка и проведение тренингов. Для эффективного внедрения программы в орган судебно-медицинской экспертизы необходимо выделить специфические требования для отдельных групп сотрудников, к которым относятся эксперты, руководство, IT-сотрудники, обслуживающий персонал, администрация, служба безопасности. Содержание тренингов следует определять в зависимости от ключевых особенностей выделенных категорий сотрудников. Периодически тренинг необходимо обновлять и дополнять, но главное – проводить его с определенной периодичностью. Для проверки уровня подготовки сотрудников можно проводить тестирование.

Третий шаг – поддержание состояния бдительности служащих. Один из методов сохранения безопасности основой мышления работника заключается в том, чтобы сделать информационную безопасность своеобразной работой, обязанностью каждого в органе. Это мотивирует сотрудника, он чувствует себя одной из частей слаженного механизма безопасности организации. Однако может возникнуть и тенденция «безопасность – не моя работа, мне за нее не платят». Программа по поддержанию бдительности должна быть как можно более интерактивной и использовать любые доступные каналы для передачи сообщений, помогающих сотрудникам постоянно помнить о хороших привычках безопасности. В процессе работы следует использовать все доступные традиционные и нетрадиционные каналы и способы. К примеру, реклама, юмор и вредные советы – традиционные способы. Использование различных слов и написаний одних и тех же сообщений-напоминаний предохраняет их от привыкания и последующего игнорирования. Список возможных действий для выполнения этой программы может включать:

- публикации статей, рассылки, напоминания, календари и даже комиксы;
- публикацию наиболее надежного работника месяца;
- специальные плакаты в рабочих помещениях;
- доски объявлений;
- печатные вкладыши в конвертах с зарплатой;
- рассылки с напоминаниями по электронной почте;
- хранители экрана и экранные заставки с напоминаниями;
- специальные наклейки на телефонах;
- системные сообщения в компьютерной сети;
- постановку вопроса безопасности одним из постоянных на собраниях, пятиминутках;
- использование локальной сети для напоминаний в картинках, анекдотах и в виде любой другой информации, которая сможет заинтересовать пользователя и прочитать текст;
- распространение буклетов и брошюр и др.

Занятия по повышению осведомленности служащих и общего уровня их знаний в области безопасности могут снизить риск подвергнуться атаке злоумышленника [5].

В органах судебно-медицинской экспертизы критически важными субъектами манипуляций с точки зрения информационно-психологической безопасности являются, в первую очередь, экс-

перты и руководство. Это связанно с тем, что именно они принимают решения, которые могут повлиять на жизнь и судьбу человека и гражданина, который не по своей воле вынужден пользоваться услугами органов судебно-медицинской экспертизы. Поэтому для них необходимо углубить тренинг, уделив внимание умению обнаруживать негативные информационно-психологические воздействия. Это умение может быть сформировано на чувственном и рациональном уровнях. Задача обучения на чувственном уровне состоит в создании особого чувственного средства обнаружения опасности. Им может стать некое ощущение, которому специально (намеренно) придается смысл средства восприятия. На рациональном уровне проводится анализ механизмов негативного информационно-психологического воздействия. Как это часто и случается, ни тот, ни другой способы сами по себе не позволяют удовлетворительно решать поставленную задачу, поэтому и необходимо изучение обоих [4].

Необходимость данной методики обусловлена родом деятельности с одной стороны, и возможностью воздействия злоумышленника именно на эти категории сотрудников, – с другой. Владея данной методикой, они смогут не только обнаружить угрозу, но и полностью избежать морального ущерба, сумев оказать достойное противодействие манипулятору. Полагаем, что обучение данной методике всех сотрудников является нецелесообразным, поскольку требует существенных затрат.

Обоснованные организационные меры должны сопровождаться разработкой как минимум трех локальных нормативных документов:

1. Перечень сведений, знание которых поможет злоумышленнику реализовать негативное информационно-психологическое воздействие, с указанием носителей этих сведений и мест их хранения;

2. Политика информационно-психологической безопасности (на основе составленного Перечня);

3. Программа тренинга сотрудников, содержащая, кроме теоретических знаний, конкретные примеры воздействий, которые могут произойти или происходили в органе, а также технологии противодействия названным воздействиям.

Заключение

Таким образом, основная угроза информационной безопасности в органах судебно-медицинской экспертизы – зависимость экспертизы, которая может быть реализована как извне – со стороны судов, судей, органов дознания, лиц, производящих дознание, следователей и прокуроров, а также иных государственных органов, организаций, объединений и отдельных лиц, так и изнутри – сотрудниками органа судебно-медицинской экспертизы. Исполнение Федеральных Законов Российской Федерации «О персональных данных» (2006) и «О государственной судебно-экспертной деятельности в Российской Федерации» (2001) требует решения проблемы обеспечения информационно-психологической безопасности сотрудников органов судебно-медицинской экспертизы. Обоснованные в настоящей статье организационные меры должны стать частью системы организационной защиты персональных данных, системы борьбы с коррупцией, а также системы кадровой работы в органах судебно-медицинской экспертизы. Внедрение этих мер может стать не только важным шагом по снижению вероятности реализации угрозы негативных информационных воздействий на сотрудников органов судебно-медицинской экспертизы с целью несанкционированного доступа к защищаемой информации, но также действенным антикоррупционным средством и одним из методов охраны труда сотрудников этих органов, гармонизации условий их профессиональной деятельности.

Литература

1. *Астахова, Л.В. Герменевтический психологический метод исследования в деятельности по обеспечению информационной безопасности: педагогический аспект / Л.В. Астахова, Т.В. Харлампьева // Вестник Челяб. гос. пед. ун-та.– 2010. – № 4.– С. 5–11.*

2. *Астахова, Л.В. Информационно-психологическая безопасность в регионе: культурологический аспект / Л.В. Астахова // Вестник УрФО. Безопасность в информационной сфере. – 2011. – № 2.– С. 40–47.*

3. Астахова, Л.В. Критическое мышление как средство обеспечения информационно-психологической безопасности личности: моногр. / Л.В. Астахова, Т.В. Харлампьева. – М.: РАН, 2009. – 141 с.

4. Астахова, Л.В. Развитие управленческой компетенции будущего специалиста по защите информации в вузе / Л.В. Астахова // Современные проблемы науки и образования. – 2012. – № 6. – С. 330.

5. Ахметвалиева, А.А. Развитие культуры информационно-психологической безопасности студентов вуза: дис. … канд. пед. наук / А.А. Ахметвалиева. – Челябинск, 2011. – 189 с.

6. Доценко, Е. Л. Психология манипуляции: феномены, механизмы и защита / Е.Л. Доценко. – М.: ЧеРо: Изд-во МГУ, 1997. – 344 с.

7. Митник, К.Д. Искусство обмана / К.Д. Митник, В.Л. Саймон. – М.: Изд-во Компания АйТи, 2004. – 360 с.

8. Федеральный закон Российской Федерации от 31 мая 2001 г. N 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации». – http://base.garant.ru/12123142

Астахова Людмила Викторовна, д-р пед. наук, профессор, профессор кафедры безопасности информационных систем, Южно-Уральский государственный университет (г. Челябинск); lvastachova@mail.ru.

Сапожников Ярослав Александрович, студент кафедры безопасности информационных систем, Южно-Уральский государственный университет (г. Челябинск); sardius@inbox.ru.

Bulletin of the South Ural State University
Series "Computer Technologies, Automatic Control, Radio Electronics"
2013, vol. 13, no. 3, pp. 122–127

THE PECULIARITIES OF A PERSONAL DATA PROTECTION IN THE BODIES FOR FORENSIC MEDICAL EXAMINATION

***L.V. Astakhova**, South Ural State University, Chelyabinsk, Russian Federation, lvastachova@mail.ru,*
***Sapozhnikov Ya.A.**, South Ural State University, Chelyabinsk, Russian Federation, sardius@inbox.ru*

The peculiarities of a personal data protection in the bodies for forensic medical examination are identified in the article. Peculiarities are associated with threats of negative information and psychological influence on the experts in the course of their professional activities. Organizational measures to address the problems of ensuring information and psychological security of the employees of the forensic medical examination, and the prospects of their introduction in practice of information protection were developed.

Keywords: personal data, information protection, information and psychological security, negative information and psychological influence, manipulation, forensic medical examination.

References

1. Astakhova L.V., Harlamp'eva T.V. Hermeneutic psychological method of research in information security activities: pedagogical aspect [Germenevticheskij psihologicheskij metod issledovanija v dejatel'nosti po obespecheniju informacionnoj bezopasnosti: pedagogicheskij aspect]. *Vestnik Cheljabinskogo gosudarstvennogo pedagogicheskogo universiteta [Bulletin of the Chelyabinsk state pedagogical University]*, 2010, no. 4, pp. 5–11.

2. Astakhova L.V. Information-psychological security in the region: the culturological aspect [Informacionno-psihologicheskaja bezopasnost' v regione: kul'turologicheskij aspekt] *Vestnik The Ural*

Federal district. Security in the information sphere [Vestnik UrFO. Bezopasnost' v informacionnoj sfere], 2011, no. 2, pp. 40–47.

3. Astakhova L.V., Harlamp'eva T.V. Critical Thinking as a Means of Ensuring Information and Psychological Security of Personality [*Kriticheskoe Myshlenie kak Sredstvo Obespechenija Informacionno-psihologicheskoj bezopasnosti Lichnosti*]. Moscow, RAS, 2009. 141 pp.

4. Astakhova, L.V. The Development of Managerial Competence of Future Specialist for the Protection of the Information in the University [Razvitie upravlencheskoj kompetencii budushhego specialista po zashhite informacii v vuze]. *Sovremennye problemy nauki i obrazovanija [Modern Problems of Science and Education]*, 2012, no. 6, p. 330.

5. Ahmetvalieva A. A. The Development of A Culture of Information-Psychological Security of the Students of the University: dis. ... kand. ped. nauk. [*Razvitie Kul'tury Informacionno-psihologicheskoj Bezopasnosti Studentov Vuza*: dis. ... kand. ped. nauk.]. Chelyabinsk, 2011. 189 pp.

6. Dotsenko, E. L. The Psychology of Manipulation: Phenomena, Mechanisms and Protection [*Psihologija Manipuljacii: Fenomeny, Mehanizmy i Zashhita*]. Moscow, CheRo, Publishing house of Moscow state University, 1997. 344 pp.

7. Mitnick K.D., Simon V.L. The Art of Deception [*Iskusstvo Obmana*]. Moscow, Publishing house of the Company services, Inc., 2004. 360 pp.

8. The Federal Law of 31 may 2001. N 73-FZ “On the State Judicial-expert activity in the Russian Federation” [*Federal'nyj Zakon Rossijskoj Federacii ot 31 maja 2001 g. N 73-FZ “O Gosudarstvennoj Sudebno-jekspertnoj Dejatel'nosti v Rossijskoj Federacii”*]. Available at: http://base.garant.ru/12123142/ (accessed 13 May 2013).

Поступила в редакцию 5 июня 2013 г.