УДК 316.354:004.056 https://doi.org/10.24158/tipor.2018.5.15

Базелюк Никита Григорьевич

ведущий инженер-программист Каспийского научно-исследовательского института рыбного хозяйства, Астрахань

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ СОЦИАЛЬНОГО УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ (НА ПРИМЕРЕ ГРУЗОВОГО ПОРТА)

Аннотация:
Современное информационное общество и деятельность социальных организаций во многом зависят от информационных ресурсов и эффективных мер по предотвращению угроз информационной безопасности. Использование распределенной обработки информации на электронных и бумажных носителях ослабляет централизованный контроль со стороны администрации и может привести к утечке или искажению информации, к информационно-психологическому воздействию на персонал предприятия. В статье на основе результатов социологического исследования на эмпирической базе грузовых портов Астраханской области обосновывается алгоритм социального управления информационной безопасностью подобных организаций, разрабатываются предложения о создании в портах служб по управлению информационной безопасностью, определяются задачи этих структур по обеспечению информационно-технической защиты информации и информационно-психологической профилактике персонала, предлагается система социального контроля за процессом обеспечения информационной безопасности предприятия.

Ключевые слова:
информационная безопасность, грузовой порт, социальный контроль, информационно-психологическое воздействие, служба по управлению информационной безопасностью, организация, управление, закон, судебная практика.

Bazelyuk Nikita Grigoryevich

Leading Software Engineer, Caspian Research Institute of Fisheries, Astrakhan

CONCERNING THE IMPROVEMENT OF INFORMATION SECURITY SOCIAL MANAGEMENT (CASE STUDY OF THE CARGO PORT)

Summary:
The modern information society and the social organizations' activities depend largely on information resources and effective measures to prevent threats to information security. The distributed processing of information on electronic and paper media weakens the administration's centralized control and can lead to leakage or distortion of information, information and psychological impact on cargo port personnel. Based on the results of a sociological survey on the empirical basis of cargo ports of Astrakhan region, an algorithm for information security social management of similar organizations is substantiated. The proposals are being developed to establish information security management services in ports; tasks of these structures for providing information technology security and information and psychological prevention of personnel are defined; a system of social control over the enterprise information security is being developed as well.

Keywords:
information security, cargo port, social control, information and psychological impact, information security management service, organization, management, law, case law.

Социологическое исследование было проведено в 2016–2017 гг. в грузовых портах Астраханской области, которые имеют уникальное географическое положение для оптимального развития торгово-экономических связей между странами Каспийского бассейна. Важной частью деятельности администраций портов являются формирование международных отношений, связанных с защитой интересов российских компаний, освоение и развитие традиционных рынков, противодействие дискриминации российских экспортеров, содействие устранению очагов напряженности. Объем выборки составил 400 человек, ошибка выборки – 4,9 %. В ходе исследования были проведены наблюдение, анкетный и экспертный опросы, интервьюирование, анализ документов, применены методы математической обработки данных.

В грузовых портах ведется электронный документооборот. «Зависимость от информационных систем и услуг означает, что организации становятся все более уязвимыми по отношению к угрозам безопасности. Тенденция к использованию распределенной обработки данных ослабляет эффективность централизованного контроля» [1].

Информационная безопасность (ИБ) грузового порта определяется как социальное явление, направленное не только на устойчивое и стабильное развитие организации, но и на повышение уровня жизни персонала, который, согласно трудовому договору, несет полную ответственность за сохранение информации, за прямой действительный ущерб, причиненный предприятию в результате нарушения правил трудового распорядка (ст. 238 Трудового кодекса РФ).

По мнению экспертов (опрошено 7 человек) грузовых портов Астраханской области, в порту действуют правила трудового распорядка, на территории отлажена пропускная система, предполагающая режим ограниченного доступа во все служебные помещения, оборудованные компьютерами и оргтехникой.

Примеры из судебной практики РФ показывают, что расследование компьютерных преступлений в судах РФ затруднено в связи с отсутствием необходимой экспертизы, которая оказывает влияние на исход судебных дел. Так, в 2013–2015 гг. в России по ст. 272 Уголовного кодекса РФ судили 459 человек. Из них, по данным «Лаборатории Касперского», только 21 преступник был приговорен к лишению свободы, так как приговор во многом зависел от компетентности судей [2].

Эксперты отмечают, что возникающие проблемы, связанные с информационно-техническим и информационно-психологическим воздействием, анализируются периодически. Основное внимание при анализе угроз ИБ уделяют технической стороне проблемы, установке антивирусных программ и т. п. Приоритетными задачами дирекция портов видит социально-экономическое развитие порта, не обращая внимания на то, что достижение целей в существенной степени зависит не только от информационной сферы и защиты информации, но и от защищенности персонала от информационно-психологического воздействия (ИПВ). В ходе данного исследования выявлено 69 % респондентов, которые испытывали на рабочем месте в портах информационно-психологическое воздействие. Инициатором ИПВ чаще становились сотрудники этого же порта (35 % респондентов). Информация из сети Интернет повлияла на состояние 22 % опрошенных. Изменение эмоционального состояния отмечено у 63 %, изменение действий и намерений – у 18 % опрошенных.

Индикатором для измерения информационно-психологического воздействия служила степень социально-экономической стабильности предприятия, отражающая соотношение групп сотрудников, с одной стороны, спокойно и сравнительно легко способных переносить трудности и готовых проявлять терпение, с другой стороны, тех, кто дальше так жить не может и требует пересмотра уровня зарплаты, режима труда и отдыха и т. п. Чем ниже уровень терпения, которое проявляют и готовы проявлять респонденты, тем сильнее угроза психологической дестабилизации персонала всего порта. Согласно результату включенного наблюдения, социально незащищенной категорией с низким уровнем терпения оказались молодые специалисты и работающие пенсионеры. Результаты опроса экспертов показали, что негативные тенденции, которые приводят к усилению дезинтеграционных явлений, связанных с информационно-психологическим воздействием, не входят в компетенции инженеров, обеспечивающих ИБ в портах.

Имеющихся в портах сил и средств недостаточно для защиты персонала от информационно-психологического воздействия. Опрос респондентов показал, что персонал грузовых портов регулярно подвергается оскорблению, моральному истязанию, психологическому давлению со стороны коллег. Конституция Российской Федерации гарантирует право граждан на судебную защиту своей чести и доброго имени (ст. 21, 23, 45, 46) [3]. Статья 5.61 Кодекса РФ об административных нарушениях предусматривает наказание за оскорбление, т. е. унижение чести и достоинства другого лица, выраженное в неприличной форме [4]. Однако администрация грузовых портов не рассматривает претензии сотрудников об оскорблении, распространении недостоверных сведений, компенсации морального вреда. По мнению 35 % респондентов, наиболее актуальной проблемой в грузовых портах Астраханской области является информационно-техническая безопасность. 10 % респондентов называют нерешенной проблему информационно-психологической безопасности. 48 % выбрали оба ответа, только 7 % назвали проблему информационной безопасности неактуальной. По мнению 42,5 % респондентов, принимать управленческие решения о необходимости социального управления информационной безопасностью затрудняет экономическая нестабильность государства. 9,75 % респондентов уверены, что одним из факторов может быть недостаточная законодательная база (рисунок 1).

Как показывают социальная практика и анализ научных публикаций [5], основными причинами отсутствия рациональных проектов по социальному управлению ИБ является политическая, экономическая и социальная нестабильность в обществе, низкая эффективность использования возможностей, сил и средств социальной базы.

В Доктрине информационной безопасности РФ представлены определения сил и средств, обеспечивающих ИБ. «Средства обеспечения информационной безопасности – правовые, организационные, технические. Силы обеспечения информационной безопасности – государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций» [6].

В Германии группа поставщиков ИТ-услуг (Vitako) инициировала разработку раздаточного материала для администраций земель и городов «Руководящие принципы для проектирования политики информационной безопасности в органах местного самоуправления», где описаны разработка и проектирование принципов информационной безопасности, способы строительства и эксплуатации систем управления информационной безопасностью государственных служащих [7]. В декабре 2015 г. в Германии был принят закон, требующий хранить метаданные клиентов (кто, где, когда, как

и с кем общался). Кредитная организация Deutsche Bank в целях повышения уровня информационной безопасности запретила сотрудникам пользоваться на рабочем месте мессенджерами (WhatsApp, СМС-сообщения), так как данные не могут быть сохранены на сервере банка [8].

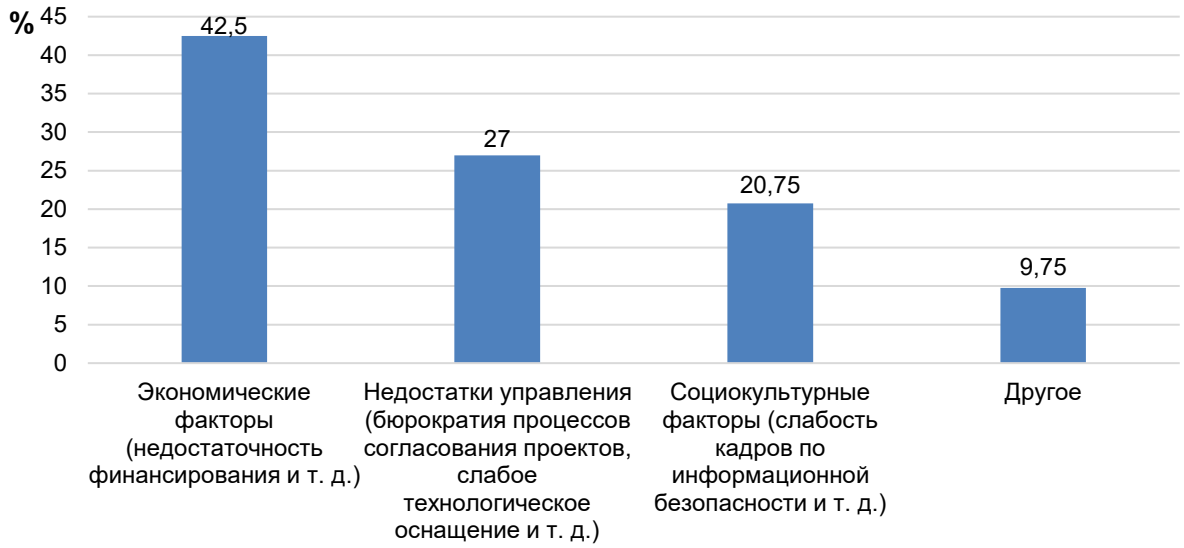

Рисунок 1 – Факторы, препятствующие социальному управлению информационной безопасностью (по мнению респондентов)

Основными инструментами неформального социального контроля за обеспечением информационной безопасности являются публичность и гласность. Как показывают наблюдения исследователя, в грузовых портах для включения механизма социального контроля ведется пропаганда здорового образа жизни, развивается корпоративная культура, в коллективе формируются определенные убеждения. На основании результатов опроса респондентов грузовых портов установлено, что в грузовом порту необходимо создать специальную службу по управлению информационной безопасностью (СУИБ), которая будет включать специалистов по техническим вопросам и программному обеспечению оборудования, а также специалистов по информационно-психологической защите персонала. СУИБ должна обеспечить информационно-техническую защиту информации и защиту психики и сознания людей от манипулирования и дезинформирования.

Силами неформального социального контроля возможно обеспечить информационную безопасность, проведя на митинге или собрании массовую агитацию с целью побуждения персонала к активным действиям, направленным на снижение дезорганизации. Осуществляя социальный контроль, сотрудники порта должны выявлять возникающие отклонения, связанные с техникой, технологией и психическим состоянием персонала; проводить упреждающие мероприятия по обеспечению ИБ и информировать персонал о проводимых мероприятиях и результатах контроля. Система информационно-психологической защиты должна строиться таким образом, чтобы своевременно пресекать распространение провокационных слухов, подавлять астенические состояния и негативные настроения.

Таким образом, принципиальными вопросами совершенствования социального управления ИБ организации является рационализация организационной системы, которая включает создание СУИБ и непрерывный характер социального контроля, принятие администрацией конструктивной и деструктивной роли информации и информационно-психологического воздействия, смещение акцента с технократических аспектов на гуманитарные.

Стратегические цели и основные направления обеспечения ИБ определены в утвержденной Президентом РФ в 2016 г. Доктрине информационной безопасности РФ. В судах РФ рассматривают дела, касающиеся нарушения порядка, сбора, хранения, использования и распространения информации. Статей, обеспечивающих информационную безопасность, связанную с угрозами информационно-технического и информационно-психологического воздействия, не предусмотрено, на законодательном уровне не закреплены наказания за моральное истязание человека или за причиненный информационно-психологический ущерб. В связи с вышеизложенным предлагаем главу 8 Гражданского кодекса РФ «Нематериальные блага и их защита» дополнить статьей 153 «Защита от информационно-психологического воздействия».

Ссылки:

1. ГОСТ Р ИСО/МЭК 17799–2005. Информационная технология. Практические правила управления информационной безопасностью [Электронный ресурс] // Консорциум «Кодекс». Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/gost-r-iso-mek-17799-2005 (дата обращения: 08.05.2018).
2. Коломыченко М. Киберпреступники сорвали банк [Электронный ресурс] // Коммерсантъ. 2015. 19 нояб. URL: https://www.kommersant.ru/doc/2857275 (дата обращения: 08.05.2018).
3. Конституция РФ [Электронный ресурс] : принята на всенар. голосовании 12 дек. 1993 г. Доступ из справ.-правовой системы «Гарант».
4. Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс] : от 30 дек. 2001 г. № 195-ФЗ : ред. от 28 дек. 2016 г. : с изм. и доп., вступ. в силу с 29 янв. 2017 г. Доступ из справ.-правовой системы «КонсультантПлюс».
5. Бачило И.Л. Гражданское общество в зеркале информационной среды // Информационное право и становление основ гражданского общества в России : материалы теор. семинара по информ. праву. М., 2008. С. 5–25 ; Гостев А.Н., Демченко Т.С. Управление информационно-психологической защитой социальной организации : монография. М., 2013. 252 с. ; Ирхин Ю.В. Роль информационных технологий во взаимодействии власти и общества (на примере Московского портала государственных услуг) // Социально-гуманитарные знания. 2014. № 6. С. 128–139.
6. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // Российская газета. 2016. 6 дек. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 08.05.2018).
7. IT-Sicherheit in Kommunalverwaltungen [Электронный ресурс] // Haufe.de. 2014. 5. Dez. URL: http://www.haufe.de/oeffentlicher-dienst/personal-tarifrecht/datensicherheit-it-sicherheit-in-kommunalverwaltungen_144_284784.html (дата обращения: 08.05.2018).
8. Deutsche Bank запретил пользоваться WhatsApp [Электронный ресурс] // Московский комсомолец: Германия. 2017. 14 янв. URL: http://www.mknews.de/articles/2017/01/14/deutsche-bank-zapretil-sotrudnikam-polzovatsya-whatsapp.html (дата обращения: 08.05.2018).

References:

Bachilo, IL 2008, ‘Civil society in the context of the information environment’, *Informatsionnoye pravo i stanovleniye osnov grazhdanskogo obshchestva v Rossii: materialy teor. seminara po inform. pravu,* Moscow, pp. 5-25, (in Russian).

‘Deutsche Bank banned WhatsApp’ 2017, *Moskovskiy komsomolets: Germaniya,* January 14, viewed 08 May 2018, <http://www.mknews.de/articles/2017/01/14/deutsche-bank-zapretil-sotrudnikam-polzovatsya-whatsapp.html>, (in Russian).

Gostev, AN & Demchenko, TS 2013, *Management of information and psychological protection of social organization,* monograph, Moscow, 252 p., (in Russian).

Irkhin, YuV 2014, ‘The role of information technologies in the interaction of government and society (a case study of Moscow public services portal)’, *Sotsial'no-gumanitarnyye znaniya,* No. 6, pp. 128-139, (in Russian).

‘IT-Sicherheit in Kommunalverwaltungen’ 2014, *Haufe.de,* 5. Dez, viewed 08 May 2018, <http://www.haufe.de/oeffentlicher-dienst/personal-tarifrecht/datensicherheit-it-sicherheit-in-kommunalverwaltungen_144_284784.html>, (in German).

Kolomychenko, M 2015, ‘Cybercriminals hit the jackpot’, *Kommersant",* November 19, viewed 08 May 2018, <https://www.kommersant.ru/doc/2857275>, (in Russian).

‘The Doctrine of Information Security of the Russian Federation’ 2016, *Rossiyskaya Gazeta,* December 06, viewed 08 May 2018, <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>, (in Russian).