УДК 316.354:004.056

Гостев Александр Николаевич

доктор социологических наук, профессор Московского государственного педагогического университета

Базелюк Никита Григорьевич

аспирант Современной гуманитарной академии

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ФЕДЕРАЛЬНЫХ ГОСУДАРСТВЕННЫХ УНИТАРНЫХ ПРЕДПРИЯТИЙ: СОСТОЯНИЕ, ПУТИ СОВЕРШЕНСТВОВАНИЯ

Аннотация:
В статье на основе результатов конкретного социологического исследования организации информационной защиты федеральных государственных унитарных предприятий (ФГУП) Астраханской области обосновывается, что информационная безопасность (ИБ) на современных ФГУП имеет значительный потенциал для совершенствования. Доказывается необходимость пересмотра состава мероприятий по защите информации, а также алгоритма их реализации; предлагаются к реализации принципы обеспечения ИБ ФГУП; утверждается необходимость создания на предприятиях отделов по ИБ.

Ключевые слова:
Астраханская область, информационная безопасность (ИБ), управление информационной безопасностью, федеральное государственное унитарное предприятие (ФГУП), отдел по информационной безопасности, социологическое исследование.

Gostev Alexander Nikolayevich

D.Phil. in Social Science, Professor, Moscow State Pedagogical University

Bazelyuk Nikita Grigoryevich

PhD student, Modern Academy for the Humanities

INFORMATION SECURITY MANAGEMENT AT FEDERAL STATE UNITARY ENTERPRISES: CONDITIONS, WAYS OF IMPROVEMENT

Summary:
Based on the results of the particular sociological research of information security organization at federal state unitary enterprises (FSUE) of the Astrakhan region, it is argued that the information security in the modern FSUEs has a significant potential for improvement. The authors prove that it is necessary to review the activities on data protection, as well as the algorithm of their implementation. The paper proposes to implement the principles of information security at the FSUEs. The authors believe that it is necessary to create information security departments in such enterprises.

Keywords:
Astrakhan region, management, information security, federal state unitary enterprise (FSUE), measures, improvement, study, security, department.

Одной из главных проблем современной организации является получение достоверной информации, а также ее хранение и защита [1, с. 98].

Практика, результаты исследований показывают, что уровень информационной безопасности (ИБ), который достигается с помощью технических средств (антивирусные программы, шифрование, криптографические методы, межсетевое экранирование и т. п.), имеет ряд ограничений и, следовательно, должен сопровождаться надлежащими организационными мерами [2, с. 37]. Кроме того, организации становятся все более уязвимыми к воздействиям оппонентов, использующих в качестве средств борьбы информационные системы [3, с. 38]. В связи с этим защита информации требует пересмотра состава мероприятий по ее обеспечению, а также качественного планирования алгоритма их реализации. Как показали результаты исследования, планирование защиты от информационно-психологических воздействий оппонентов должно осуществляться на трех основных уровнях: стратегическом, оперативном и тактическом [4, с. 237].

Исследование на опытной базе ФГУП (N = 5) показало, что в сфере защиты информации система управления неэффективно работает по обеспечению реализации политики ИБ. Например, персонал ФГУП недостаточно осведомлен о случаях атак на информационные системы, хищения информации, о вреде и последствиях утечки информации. Так, опрос сотрудников ФГУП Астраханской области показал, что 56,8 % респондентов затруднились с ответом на вопрос о проводимых мероприятиях по ИБ. Наблюдения показали, что в настоящее время организационные мероприятия на ФГУП в основном состоят из бесед с сотрудниками подразделений с целью ознакомления с Уставом и правилами работы с информацией, приказами. В трудовом договоре отдельными пунктами оговаривается запрет на разглашение конфиденциальной информации. Однако на ФГУП не уделяется должного внимания проблеме доступа к конфиденциальной информации сотрудников внешних организаций, которые по каким-либо причинам получили возможность ознакомиться с информационными ресурсами.

Безусловно, полная закрытость организации ограничивает взаимодействие с внешними агентами. Как известно, социальное взаимодействие людям необходимо для быстрого, рационального и достаточного для существования удовлетворения потребностей и интересов [5, с. 92]. По сути, это одна из основных проблем социального управления информационной безопасностью ФГУП, которое призвано формировать «организационные механизмы совместной деятельности людей для создания лучших условий жизнедеятельности» [6, с. 110].

Изучение практики ФГУП показывает, что решать проблему ИБ необходимо, основываясь на комплексном подходе к организации социального управления и следуя известным принципам деятельности. Один из них – разумное соотношение материальных затрат на защиту информации и возможных материальных потерь в результате утечки информации. Важно и то, какие затраты должен понести злоумышленник, чтобы «вскрыть» систему, и как они соотносятся с ценностью собранной и охраняемой информации. В связи с этим организационные мероприятия по обеспечению ИБ ФГУП должны планироваться на основании нескольких принципов: коллективной и индивидуальной ответственности; прозрачности контроля; объективности; полной подотчетности; документирования результатов деятельности; координации работы на всех уровнях управления.

Изучение действенности системы ИБ ФГУП показало, что в ней должен быть создан резерв как программно-технических средств, так и дублирующих процедур обеспечения безопасности. Исследование позволило выявить факт низкого уровня вовлеченности сотрудников предприятий в решение проблем ИБ. Так, почти весь персонал ФГУП (97 % респондентов) никогда не принимал участия в обсуждении внутрикорпоративных документов, регулирующих деятельность по обеспечению ИБ. В связи с этим назрела необходимость создания на предприятии отдела по информационной безопасности, который будет профессионально организовывать мероприятия по обеспечению ИБ. Результаты опросов показали, что большинство сотрудников ФГУП Астраханской области (79,25 %) солидарны с этим выводом (см. рис. 1).

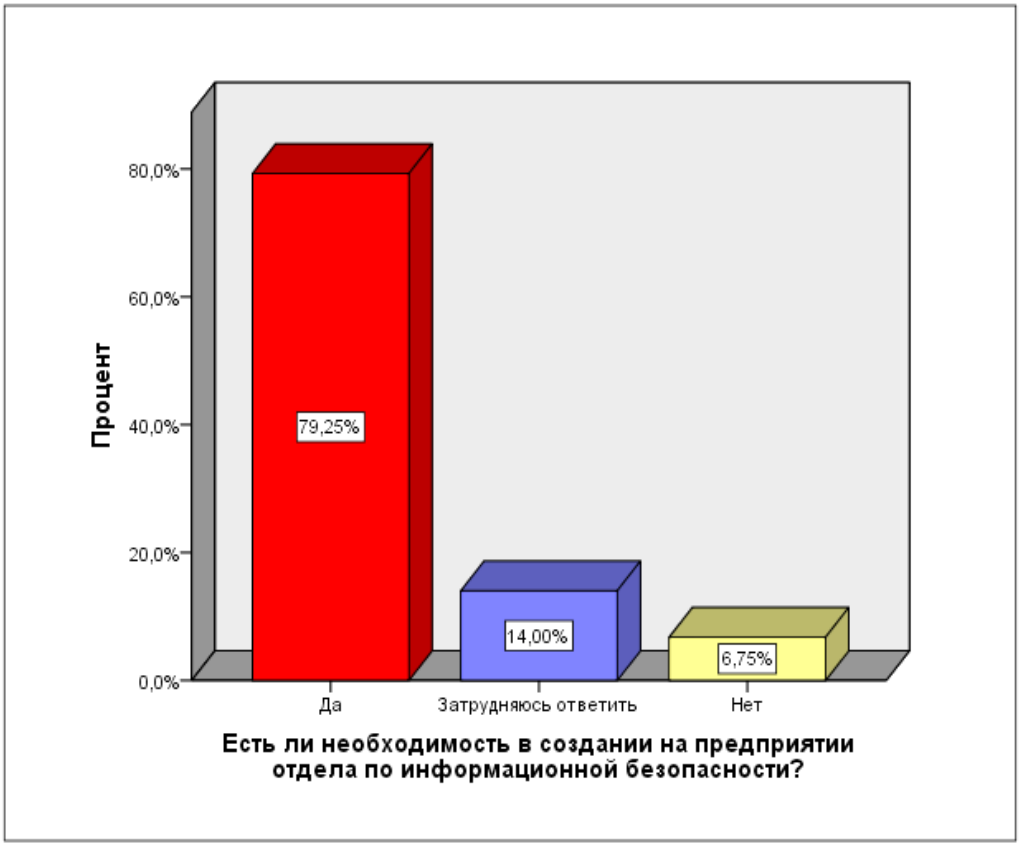

Рисунок 1 – Мнение персонала о создании на предприятии отдела по информационной безопасности

В результате изучения состояния дел по обеспечению ИБ ФГУП выявлено, что необходим новый алгоритм организации ИБ ФГУП. Очевидно, что мероприятия ИБ должны быть спланированы специалистами по информационной безопасности, затем вынесены на обсуждение с заинтересованными и ответственными за работу в этой сфере сотрудниками, утверждены руководителем и доведены до сведения всех сотрудников в доступной и понятной форме.

Результаты анализа научной литературы [7; 8; 9; 10; 11; 12; 13; 14; 15; 16] показывают, что алгоритм организации управления ИБ включает следующие этапы: оценку угроз и опасностей информационных воздействий; целеполагание; прогнозирование; проектирование; программирование, планирование; подбор и формирование команды исполнителей; отбор персонала для работы с закрытой информацией; организацию деятельности по защите информации; организацию контроля; коррекцию, уточнение процедуры деятельности и штата исполнителей [17, с. 25]. Анализ сложившейся на ФГУП практики показывает, что деятельность по обеспечению ИБ организовывается в соответствии с нормативной правовой базой и договорными обязательствами. Уточнение нормативных документов по обеспечению ИБ на предприятиях осуществляется в соответствии с годовым графиком или по необходимости, исходя из количества зарегистрированных нарушений в сфере ИБ.

Предполагается, что специалисты отдела по ИБ ФГУП должны будут налаживать контакты с другими предприятиями внутри своего ведомства, чтобы быть в курсе отраслевых тенденций по обеспечению ИБ и адекватно реагировать на инциденты, связанные с нарушением ИБ. В функции сотрудников отела информационной безопасности будет входить разработка программ обучения персонала работе с внутриведомственной информацией, нормативных требований безопасности в процессе обработки и использования информации, профилактических мероприятий, связанных с возможной утечкой информации.

Таким образом, можем сделать вывод о том, что информационная безопасность на современных ФГУП имеет значительный потенциал для совершенствования. Защита информации требует пересмотра состава мероприятий, а также планирования алгоритма их реализации. Мероприятия по обеспечению информационной безопасности ФГУП должны осуществляться по принципам коллективной и индивидуальной ответственности, прозрачности контроля, объективности, полной подотчетности, документирования результатов деятельности, координации работы на всех уровнях управления. Необходимым является создание на предприятиях отделов по информационной безопасности.

Ссылки:

1. Гостев А.Н., Демченко Т.С. Управление информационно-психологической защитой социальной организации : монография. М., 2013. 224 с.
2. Гостев А.Н. Войны XXI в.: проблема подготовки населения // Социология образования. 2012. № 12а. С. 30–43.
3. Общественный контроль производственных компаний: система протестных форм / В.М. Ананишнев, А.Н. Гостев, С.С. Демидова, Т.С. Демченко // Системная психология и социология. 2015. № 16. С. 34–39.
4. Гостев А.Н. Социально-психологическая подготовка населения страны к отражению возможной агрессии : монография. М., 2003. 504 с.
5. Гостев А.Н., Демченко Т.С. Гражданское общество: контроль над деятельностью государства : монография. М., 2011. 193 с.
6. Гостев А.Н. Общественный контроль производственных компаний // Вестник Адыгейского государственного университета. Серия «Регионоведение: философия, история, социология, политология, культурология». 2015. С. 108–116.
7. Ананишнев В.М. Социология образования : монография. М., 2008. Т. 2. 204 с.
8. Бокарева В.Б. Социальное управление внешней и внутренней средой предприятия малого бизнеса в России // Известия Уральского государственного университета. Серия 3: Общественные науки. Екатеринбург, 2012. № 1 (100). С. 112–120.
9. Гостев А.Н. Социально-психологическая подготовка …
10. Гостев А.Н., Демченко Т.С. Гражданское общество …
11. Гостев А.Н., Демченко Т.С. Управление информационно-психологической защитой …
12. Гостев А.Н. Войны XXI в. …
13. Демченко Т.С. Качество обучения в высших учебных заведениях как объект социального контроля // Труды СГА. М., 2009. Вып. 8 (август). С. 125–135.
14. Саблуков А.В. Общественное мнение как инструмент социальной экспертизы в сфере образования // Право и образование. 2013. № 7. С. 41–56.
15. Сакович С.М. Роль информационных и коммуникационных технологий в обеспечении качества и доступности высшего социологического образования // Вестник Московского государственного областного университета. 2010. № 3. С. 40–45.
16. Романова Е.С. Родительская общественность в решении образовательной политики / Е.С. Романова, Б.М. Абушкин, А.В. Ткаченко // Системная психология и социология. 2014. № 2 (10). С. 37–45.
17. Гостев А.Н. Атака на сознание (Об активизации социально-психологической подготовки населения страны и его защиты в условиях возможных военных действий) // Армейский сборник. 2004. № 2. С. 23–27.

References:

1. Gostev, AN & Demchenko, TS 2013, *Office of Information and psychological protection of social organization*: monograph, Moscow, p. 224.
2. Gostev, AN 2012, 'War of XXI century .: the problem of training people', *Sociology of Education*, no. 12a, pp. 30-43.
3. Ananishnev, VM, Gostev, AN, Demidova, SS & Demchenko, TS 2015, 'Public control of production companies: the system of protest forms', *Systemic psychology and sociology*, no. 16, pp. 34-39.
4. Gostev, AN 2003, *Socio-psychological training of the population to repel possible aggression*: monograph, Moscow, p. 504.

5. Gostev, AN & Demchenko, TS 2011, *Civil society: control over the activity of the state*: monograph, Moscow, p. 193.
6. Gostev, AN 2015, 'Public control of production companies', *Herald of Adygeya State University. A series of "Regional: philosophy, history, sociology, political science, cultural studies,*" pp. 108-116.
7. Ananishnev, VM 2008, *Sociology of Education*: monograph, Moscow, vol. 2, p. 204.
8. Bokareva, VB 2012, 'Social management of the external and internal environment of small business in Russia', *Proceedings of the Ural State University. Series 3: Social Sciences*, Ekaterinburg, no. 1 (100), pp. 112-120.
9. Gostev, AN 2003, *Socio-psychological training of the population to repel possible aggression*: monograph, Moscow, p. 504.
10. Gostev, AN & Demchenko, TS 2011, *Civil society: control over the activity of the state*: monograph, Moscow, p. 193.
11. Gostev, AN & Demchenko, TS 2013, *Office of Information and psychological protection of social organization*: monograph, Moscow, p. 224.
12. Gostev, AN 2012, 'War of XXI century .: the problem of training people', *Sociology of Education*, no. 12a, pp. 30-43.
13. Demchenko, TS 2009, 'The quality of teaching in higher education as an object of social control', *Proceedings of the SGA*, vol. 8 (August), Moscow, pp. 125-135.
14. Sablukov, AV 2013, 'Public opinion as an instrument for social assessment in education', *Law and Education*, no. 7, pp. 41-56.
15. Sakovich, SM 2010, 'The role of information and communication technologies to ensure the quality and accessibility of higher education Sociological', *Bulletin of Moscow State Regional University*, no. 3, Moscow, pp. 40-45.
16. Romanova, ES, Abushkin, BM & Tkachenko, AV 2014, 'The parent community in addressing educational policy', *Systemic psychology and sociology*, no.2 (10), pp. 37-45.
17. Gostev, AN 2004, 'The attack on the consciousness (about intensification of socio-psychological training of the country and protect the population in the conditions of possible military action)', *Army collection*, no. 2, pp. 23-27.