Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

правляются специальными либо курьерскими почтовыми отправлениями (в исключительных случаях, если государственный орган или иная организация не являются пользователями услуг специальной связи или курьерских услуг, - заказными почтовыми отправлениями) с соблюдением требований по защите государственных секретов.

Порядок учета, хранения, использования и уничтожения информационных ресурсов, содержащих конфиденциальные сведения, а также порядок выдачи из таких информационных ресурсов указанных сведений определяются соответственно Министерством внутренних дел, Комитетом государственной безопасности, Государственным пограничным комитетом, Службой безопасности Президента Республики Беларусь, Оперативно-аналитическим центром при Президенте Республики Беларусь, Комитетом государственного контроля, Государственным таможенным комитетом и Министерством обороны.

Конфиденциальные сведения государственным органам, иным организациям и гражданам не предоставляются.

Если основанием для применения мер безопасности является постановление о применении мер безопасности, вынесенное должностным лицом органа, осуществляющего оперативно-розыскную деятельность, или процессуальное постановление органа, ведущего уголовный процесс, о результатах проверки информации об истребовании сведений о защищаемом лице в связи с производством по уголовному делу, орган, обеспечивающий безопасность, уведомляет принявший решение о применении мер безопасности орган, осуществляющий оперативно-розыскную деятельность, или орган, ведущий уголовный процесс, для решения вопроса о предоставлении запрашиваемых сведений или об отказе в их предоставлении.

Сводные данные о применении мер безопасности и реализации мер социальной защиты не должны содержать сведений, позволяющих определить принадлежность персональных данных защищаемому лицу.

Список литературы

1. Кодекс Республики Беларусь от 16.07.1999 № 295-З (ред. от 20.04.2016) "Уголовно-процессуальный кодекс Республики Беларусь".

2. Кодекс Республики Беларусь от 09.07.1999 № 275-З (ред. от 19.07.2016) "Уголовный кодекс Республики Беларусь".

3. Постановление Совета Министров Республики Беларусь от 21.01.2016 № 44 (ред. от 02.12.2016) "Об утверждении Положения о порядке применения мер безопасности в отношении защищаемых лиц".

4. Решение Конституционного Суда Республики Беларусь от 29.12.2015 № Р-1024/2015 "О соответствии Конституции Республики Беларусь Закона Республики Беларусь "О внесении изменений и дополнений в некоторые кодексы Республики Беларусь".

ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

В.Б. СОКОЛОВ

Белорусский государственный университет информатики и радиоэлектроники

Человечество жило в век пещер и мамонтов, в каменном, бронзовом и железном веке. Теперь же человечество живет в веке информации. Информация того или иного рода является неотъемлемой частью нашей жизни. Именно информация является доми-

нирующим фактором в нашей жизни, тем фактором, который определяет не только уровень жизни каждого человека, но и экономику, обороноспособность, политическую стабильность любого государства. Как следствие – защита информации является одним из приоритетных направлений как государственной экономики, так и политики [1].

Сейчас практически не осталось ни одной организации либо предприятия, которые бы не использовали в своей работе разнообразные информационные системы, начиная от единичных персональных компьютеров и заканчивая сетевыми системами с выходом в Интернет. Нарушение безопасности этих систем даже на непродолжительное время способно остановить работу предприятия и нанести существенный ущерб. Информационная безопасность важна и для каждого человека, ведь ее нарушение способно нанести непоправимый как моральный, так и материальный вред.

В таких условиях особое значение приобретает подготовка кадров в области защиты информации. К сожалению, эта подготовка оставляет желать лучшего во многих аспектах, начиная от низкого уровня подготовки абитуриентов и заканчивая отсутствие отбора по моральным и психологическим качествам [2].

Следует заметить, что практически во всех высших учебных заведениях, которые занимаются подготовкой кадров в области информационной безопасности, не только не производится начальный отбор будущих специалистов исходя из психологических и моральных требований, но и в процессе обучения не проводится корректировка психологического и морального состояния студентов [3].

Дело в том, что специалисты в области информационной безопасности должны, кроме высокой профессиональной компетентности, обладать рядом качеств, наличие или отсутствие которых может оказаться критичным для успешности их работы. Так, имеющиеся у многих абитуриентов детские психологические травмы могут помешать им в дальнейшем, если не будут нивелированы с помощью специалистов. Например, наличие комплекса неполноценности может привести к тому, что будущий специалист по информационной безопасности пожелает доказать окружающим свою ценность и значимость. Подобное доказательство может вылиться в крайне неприятные с профессиональной точки зрения формы: хакерская атака («Посмотрите, какой я умный!»), разглашение конфиденциальных сведений, передача конфиденциальных сведений конкурирующей организации и так далее. Причем, это только комплекс неполноценности, а ведь в современном мире великое множество различных психологических травм, и не все они совместимы с некоторыми видами работ. Но почему-то все понимают, что инвалид не может заниматься тяжелым физическим трудом, однако не желают воспринимать тот факт, что психологические проблемы могут привести не только к неудачам в личной жизни или частной профессиональной несостоятельности, но при некоторых профессиях (к которым относится обеспечение информационной безопасности) оказаться буквально опасными для общества.

Интересны данные итальянских психологов, которые занимались исследованием в области информационной безопасности. Оказывается, в среднем 25 % служащих практически любой организации или предприятия являются действительно надежными людьми. Еще 25 % ждут удобного случая или выгодного предложения, чтобы разгласить конфиденциальную информацию, ну а остальные 50 % могут быть как преданными людьми, так и разгласить секреты организации – в зависимости от обстоятельств (к примеру, насколько щедрым будет предложение оплаты секретов фирмы) [4].

Но эта статистика относится и к специалистам по информационной безопасности, так как они не проходят специальную психологическую подготовку. В результате они так же, как и все остальные, разделяются на 25 % искренне преданных своему делу, 25 % потенциальных, а то и реальных представителей пятой колонны и 50 % колеблющихся в ту сторону, которая на данный момент окажется выгоднее.

В таких условиях возникает резонный вопрос: кто будет контролировать контролеров? Или: кто будет защищать информацию от защитников? Возможно, гораздо более эффективным будет не контролировать и/или защищать, но соответствующим образом готовить специалистов по информационной защите, причем, далеко не только с технической точки зрения, но обязательно учитывая и психологическую составляющую.

Необходимо учитывать, что защита информации – это далеко не только техники и технологии, это в первую очередь человек, который является в этой системе самым слабым звеном в силу своей неопределенности. Человек – не машина, и его действия не всегда являются предсказуемыми и логичными. Однако те, кто занимается обеспечением информационной безопасности, как раз должны быть и логичны, и предсказуемы – по крайней мере в поведенческом аспекте. В то же время они должны обладать творческим складом ума, чтобы эффективно справляться с изменяющимися воздействиями на информационную среду.

В студентах, обучающихся на специальностях, связанных с информационной защитой, необходимо культивировать следующие качества: верность, преданность, чувство долга. Они должны быть уверены в себе, достаточно самостоятельны, чтобы заниматься самообразованием, а также принимать решения в различных, в том числе и критических ситуациях (иногда обеспечение информационной безопасности требует известной оперативности в принятии решения, и нет времени для «консультаций со специалистами» или для «доклада начальству»).

Самостоятельность как черта характера предполагает еще и то, что человек не последует за лидером в том случае, если этот лидер предлагает нечто, несовместимое с убеждениями либо даже прямое нарушение обязательств перед работодателем, а то и законодательством. То есть, для специалиста по информационной безопасности не должны действовать установки: «буду воровать потому, что воруют все», «если не украсть, то не прожить», «нельзя жить на одну зарплату» и так далее. Все установки такого типа особенно эффективно действуют при наличии харизматичного лидера и склонности к бездумному подчинению, как удобной системы существования (как писал К. Чапек: «Овца: пусть зарежут, лишь бы вели!»). Специалисты в области защиты информации не должны обладать психологическими качествами овцы, напротив, они сами должны проявлять качества харизматичного лидера с возможностью увлекать других людей к неким горизонтам (например, уметь заражать своей преданностью делу, желанием узнавать новое и так далее).

Для специалистов этой области психологическая стабильность необходима, поэтому для них существенным фактором является наличие семьи, при этом желательно два-три ребенка. В то же время стремление к стабильности не должно перерастать в стремление к стереотипности, ведь наш мир стремительно изменяется, и обеспечение безопасности информации связано с постоянным изменением как технологий, так и техники, которые эту информацию обеспечивают. Так что специалисты по информационной безопасности должны обладать здоровым любопытством и постоянным стремлением к новым знаниям, новым горизонтам.

Необходимо заметить, что стремление к образованию в течение всей жизни является обязательным условием для компетентного специалиста в области информационной безопасности. Отсутствие побудительной мотивации к образованию приводит не просто к застою мысли, но к быстрой потере квалификации в динамичном и достаточно неопределенном мире: фактически ежедневно появляются новые источники опасности для информационного поля, новые «сорняки», для которых необходимо разрабатывать и применять новые методы воздействия и «прополки» [5]. Если же специалист предпочитает довольствоваться традиционными и – что важно! – неизменными методами, то это может привести к неэффективности его деятельности и, как следствие, к значительным потерям для организации, в которой такой специалист работает.

В условиях стремительной изменчивости окружающей среды оказывается, что техническая подготовка специалистов по защите информации больше заключается в формировании и развитии у них творческого и самостоятельного мышления, чтобы они продолжали стремиться к новым знаниям постоянно, даже после получения диплома о высшем образовании, а также в обучении умению пользоваться разнообразной справочной и научной литературой, что впоследствии поможет осваивать новые техники и технологии. В то же время психологическая подготовка приобретает все большее значение: чем больше и стремительнее изменяется техника, тем больше требуется психологической стабильности, «якоря», чтобы не только не утонуть в информационном море, но и иметь возможность контролировать его, управлять им.

Специалисты в области информационной безопасности должны обладать следующими качествами: высоким интеллектом, способностью и желанием к творческому мышлению, способностью к выполнению нестандартных задач, стремлением к постоянному совершенствованию, психологической устойчивостью, способностью к сосредоточению внимания (в том числе и к длительному), упорством в целедостижении.

Пытаясь создать квалифицированного специалиста по информационной защите, мы неизбежно приходим к выводу, что для этого требуются комплексные усилия как преподавательского состава высших учебных заведений, так и профессиональных психологов, которые должны обеспечить необходимые личностные качества студентов данных специальностей.

Список литературы

1. Авсентьев О.С., Прийма В.Н., Малышев А.А., Дураковский А.П. Системные аспекты проблематики подготовки специалистов в области информационной безопасности. // Информационная безопасность. – 2009. - № 4. – с. 621-622.

2. Козачок А.И. Проблемы реализации компетентного подхода при подготовке специалистов по защите информации. // Ученые записки Орловского государственного университета. – 2013. - № 2 (52) – с. 294-297.

3. Кравцов А.А. Специфика профессиональной подготовки студентов по направлению «Информационная безопасность» // Вестник МГЛУ. – 2013. – Выпуск 16 (676). – с. 137-149.

4. Черкасов В. Н. Бизнес и безопасность. Комплексный подход. М.: Армада-пресс, 2001

5. Чванова М.С., Анурьева М.С., Лыскова В.Ю., Котова Н.А., Молчанов А.А. Подготовка специалистов в области информационной безопасности: инновационный подход к формированию образовательной среды. // Психолого-педагогический журнал Гаудеамус, № 1, 2015. – с. 18-31.