УДК 004.056
ББК 73
К – 38

Киздермишов Асхад Асланчериевич, *кандидат физико-математических наук, доцент кафедры организации и технологии защиты информации факультета новых социальных технологий Майкопского государственного технологического университета, тел.:(8772)538362*

СНИЖЕНИЕ РИСКА ВОЗНИКНОВЕНИЯ ПРЕДПОСЫЛОК УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СВЯЗАННЫХ С ОШИБОЧНЫМИ ДЕЙСТВИЯМИ И НЕВЕРНО ПРИНЯТЫМИ РЕШЕНИЯМИ СПЕЦИАЛИСТОВ ОТВЕТСТВЕННЫХ ЗА ЗАЩИТУ ИНФОРМАЦИИ

(рецензирована)

Разработка рекомендаций по снижению риска возникновения предпосылок угроз информационной безопасности, связанных с проблемой комплексности подхода к обеспечению защиты информации в организациях, учреждениях, фирмах, в условиях отсутствия штатных специалистов по защите информации.

Ключевые слова: информационная безопасность, защита информации.

***Kizdermishov Askhad Aslancherievich**, candidate of physical and mathematical sciences, associate professor of the chair of organization and technology of information protection of the faculty of new social technologies, Maikop State Technological University, tel.: (8772) 538362*

REDUCING THE RISK OF THE PREREQUISITES OF INFORMATION SECURITY THREATS BECAUSE OF MISLEADING AND INCORRECT DECISIONS OF SPECIALISTS RESPONSIBLE FOR DATA PROTECTION

Recommendations for reducing the risk of the prerequisites of information security threats related to the problem of an integrated approach to information security in organizations, institutions, companies, in the absence of professional staff to protect information have been developed.

Keywords: information security, information protection

Основной принцип защиты информации – комплексность, предполагает решение задач информационной безопасности проведением комплекса технических, организационных и правовых мероприятий. Приобретение и установка даже самых дорогих и современных технических средств защиты информации не защитит информацию, если не проведены организационно-правовые мероприятия: персонал не предупрежден об ответственности за нарушение режима секретности и не обучен правилам работы со средствами защиты, в действиях персонала и администраторов нет системы, направленной на обеспечение защиты информации и т.п.

Отсутствие комплексного подхода создает серьезные предпосылки для возникновения угроз информационной безопасности. Как показывает мировой опыт, абсолютное большинство случаев потери информации, в том числе в результате атак, связано с неверными действиями (ошибками) и небрежностью персонала самих компаний (фирм). Очевидно, что проблема с неверными действиями и принимаемыми решениями по защите информации особенно актуальна для фирм, в которых нет штатных специалистов по защите информации. В основном это небольшие предприятия, офисы или обособленные территориальные подразделения государственных учреждений, с небольшой штатной численностью или низкой заработной платой, что не позволяет им обеспечивать свою информационную безопасность силами штатных специалистов. В

соответствии с общепринятой практикой, в случае отсутствия штатного специалиста (подразделения) по защите информации, приказом руководителя назначается ответственный специалист по защите информации. Как правило, это специалист в области информационных технологий, а иногда и работник никогда ранее не имевший отношения к защите информации, на которого в дополнение к основным функциональным обязанностям возлагается ответственность за проведение мероприятий по защите информации. Следует отметить, что не существует никаких нормативных или руководящих документов определяющих требования к квалификации, процедуру и возможность назначения того или иного работника ответственным специалистом по защите информации (далее ОСЗИ). Безусловно, ОСЗИ положительно влияют на общую ситуацию по защите информации, однако, именно они наиболее склонны к принятию узко специализированных решений, характерных для опыта их предыдущей работы. Очевидно, что для снижения риска возникновения предпосылок угроз информационной безопасности, связанных с ошибочными действиями и неверно принятыми решениями ОСЗИ, необходимо повышать их квалификацию всеми известными способами (курсы повышения квалификации, самоподготовка, аттестация и т.п.). Однако, разработки в области повышения квалификации ОСЗИ крайне редко учитывают специфику работы в малых фирмах и обособленных подразделениях, а именно не акцентируют внимание на характерных для этой категории работников направлениях обучения, которые сбалансируют их знания технической, организационной и правовой составляющих деятельности по защите информации именно в том соотношении, которое позволит им видеть решение поставленных задач в проведении комплекса мероприятий, и, следовательно, принимать именно комплексные решения по информационной безопасности. Только оказывая такую помощь ОСЗИ, как приведение их знаний в правовой, организационной и технической защите информации к единому комплексу навыков и умений, мы сможем устранить предпосылки угроз информационной безопасности связанных с ошибочными действиями и неверно принятыми решениями. Таким образом, при разработке методик повышения квалификации ОСЗИ объектом изучения должен являться: результат сравнения неформализованной модели ОСЗИ и модели профессионального специалиста по защите информации. Только с учетом выявленных расхождений двух этих моделей, можно разработать методику, компенсирующую недостающие сегменты в знаниях ОСЗИ, что позволит повысить эффективность самообучения, самоаттестации и курсов повышения квалификации для ОСЗИ, а так же подготовки предложений конкурсных комиссий и менеджеров при приеме на работу служащих (специалистов) и эффективность самоподготовки соискателей к участию в конкурсе на замещение вакантных должностей в государственных учреждениях.

Для достижения этой цели в первую очередь необходимо построить неформализованную модель профессионального специалиста по защите информации. Под моделью знаний будем понимать распределение объема изученного специалистом материала по всем аспектам комплекса мероприятий по защите информации: техническое, организационное и правовое направления. Модель знаний специалиста по защите информации (далее МЗС) строим исходя из предположения, что количество часов, в соответствии с Государственным образовательным стандартом высшего профессионального образования по специальности 075300 «Организация и технология защиты информации», на изучение дисциплины соответствует объему изучаемого материала. Современные специалисты по защите информации должны обладать широким спектром знаний, однако считаем, что для построения МЗС достаточно исследовать основные направления деятельности по защите информации.

Следующая задача найти открытые информационные ресурсы и провести анализ содержащейся в них информации по таким критериям как: направленность, популярность, объем, угрозы для информационной безопасности в результате распространения этой

информации, на основе этого анализа построить неформализованную модель знаний непрофессионального специалиста по защите информации.

Задача построения неформализованной модели знаний специалиста по защите информации (без профессионального образования) представляется более сложной. Единственное решение - в роли ГОСТа, который мы использовали для МЗС, использовать список литературы, которую изучают ОСЗИ.

Во-первых, необходимо определить какую именно литературу изучают ОСЗИ. Следует отметить, что провести полностью объективное и достоверное исследование не представляется возможным. Однако, используя некоторые приближения, можно провести качественную оценку соотношения изучаемой литературы по всем аспектам комплекса мероприятий по защите информации: техническое, организационное и правовое направления. Например, проанализировав рейтинги продаж Интернет - магазинов мы получим модель аналогичную МЗС. Другими словами сможем оценить соотношение между сегментами по технической, организационной и правовой защите информации, изложенными в изучаемой литературе, с учетом необходимости обеспечения всего комплекса мероприятий по защите информации и единственно эффективного комплексного подхода к решению задач по информационной безопасности. На самом деле построенная таким образом МЗСБ, справедлива только для ОСЗИ, которые добросовестно и с достаточной степенью настойчивости изучают весь представленный на открытых информационных ресурсах материал.

Очевидно, что возможно уточнить построенную МЗСБ. Исходя из предположения, что студенты оказывают существенное влияние на рейтинг книг относящихся к учебным пособиям, и не оказывают существенное влияние на рейтинг остальных книг (пользуются библиотеками ВУЗов, так как эти книги не нужны им «каждый день»), а также что ОСЗИ не приобретают учебники для ВУЗов, для исключения вклада студентов в рейтинги книг необходимо исключить из рейтингов учебные пособия. Это предположение можно проверить, сравнив рейтинг учебных пособий с МЗС. Полученные результаты для неформализованной модели ОСЗИ, не являются неожиданными, на практике в абсолютном большинстве случаев именно специалисты в области информационных технологий (технические специалисты) назначаются ОСЗИ, как наиболее подготовленные к проведению технических мероприятий по защите информации.

Будем считать, что лучший результат, полученный ОСЗИ в ходе самостоятельного изучения дисциплин, может соответствовать требованиям Государственного образовательного стандарта высшего профессионального образования по специальности 075300 «Организация и технология защиты информации», таким образом, максимальное значение объема знаний ОСЗИ соответствует значению объема знаний профессионального специалиста по защите информации по соответствующей дисциплине. Тогда для построения можно представить МЗСБ в единицах МЗС (см. рисунок 1)

Из сравнения следуют существенные отличия МЗС и МЗСБ. Во-первых, у МСЗБ в отличие от МЗС отсутствует плавный переход между сегментами, что свидетельствует о наличии у ОСЗИ обрывочных знаний без увязки по комплексу направлений деятельности по защите информации. Во-вторых, общий объем знаний ОСЗИ уступает общему объему знаний профессионального специалиста по защите информации, а по направлениям организационной и правовой деятельности объем знаний ничтожно мал, что, очевидно, может привести к возникновению предпосылок угроз информационной безопасности, связанных с ошибочными действиями и неверно принятыми решениями. Из проведенного расчета следует, что для ОСЗИ вероятность не совершения ошибок и принятия верного решения по проведению комплекса мероприятий по защите информации включающего в себя как технические, так и организационно- правовые направления деятельности, равна 0,06 % .

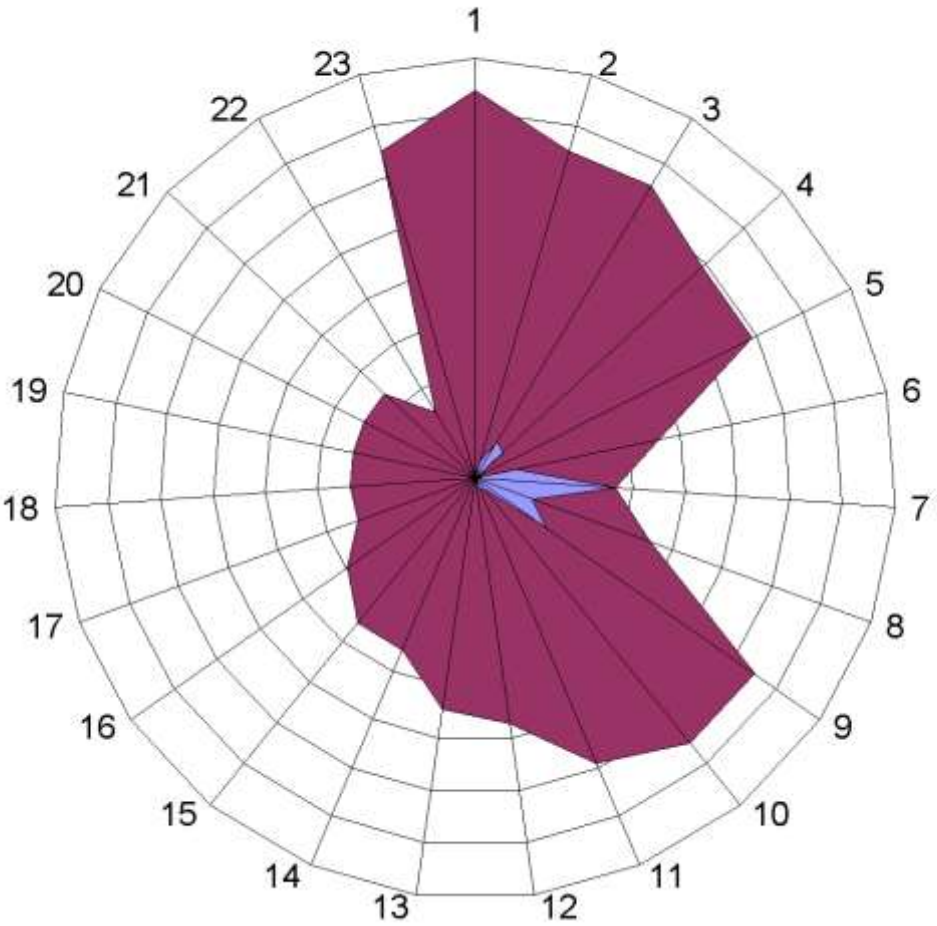

Рис.1 Сравнение МЗС и МЗСБ, внутренняя область – МСЗБ, внешняя область МЗС в единицах МЗСБ. Сегменты 1-8 техническое направление, 10-22 организационное направление, 23 – правовое направление.

Заключение.

В работе исследована проблема комплексности подхода к обеспечению защиты информации в организациях, учреждениях, фирмах, в условиях отсутствия штатных специалистов по защите информации. В результате исследования получены следующие результаты:

1. Выявлены существенные отличия в моделях знаний профессиональных и непрофессиональных защитников информации. Установлено, что область знаний специалистов, не получивших высшее профессиональное образование по защите информации, в основном соответствует техническому направлению и ничтожна мала по организационному и правовому направлениям комплекса мероприятий по защите информации, что, очевидно, может привести к возникновению предпосылок угроз информационной безопасности.

2. Специалист без профессионального образования по защите информации используя открытые информационные ресурсы и общедоступную литературу для самообразования не способен выполнить комплекс мероприятий по защите информации, включающий в себя техническое, правовое и организационное направление деятельности с той же эффективностью, что и профессиональный специалист по защите информации, получивший высшее образование в соответствии с Государственным образовательным стандартом высшего профессионального образования по специальности 075300 «Организация и технология защиты информации». Эффективность деятельности

непрофессионального защитника информации по сравнению с профессиональным составляет менее одной десятой процента. Полученный результат не является очевидным, так как при исследовании учитывалась специфика деятельности непрофессионального защитника информации, а именно небольшой объем выполняемых мероприятий по информационной безопасности и совмещение обязанностей по защите информации с основными профессионально исполняемыми функциональными обязанностями.

3. Открытые информационные ресурсы содержат информацию по всем направлениям обеспечения комплекса мероприятий по защите информации, однако, высокой популярностью пользуются только техническое направление деятельности.