

ОБРАЗОВАТЕЛЬНЫЕ ПОТРЕБНОСТИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Б.А. Швырев, канд. физ.-мат. наук, вед. науч. сотр.
ФКУ Научно-исследовательский институт ФСИН России
(Россия, г. Москва)

DOI: 10.24411/2500-1000-2019-10852

***Аннотация.** Рассматривается актуальность образования по направлению «Информационная безопасность». Выявляется потребность в специалистах со среднетехническим образованием. Определяются педагогические подходы для восполнения знаний у практиков. Отмечается важность непрерывного образования в вопросах информационной безопасности. Эффективность обучения информационной безопасности может быть достигнута в результате творческого подхода к выбору разнообразных методов и приемов, которые практикующие специалисты должны адаптировать каждый раз к обучаемой аудитории для получения максимальной положительной ответной реакции.*

***Ключевые слова:** обучение информационной безопасности, непрерывное обучение, информационно-разъяснительная работа.*

«Информационная безопасность», «Обучение информационной безопасности» и «Осведомленность и конфиденциальность» в настоящее время являются актуальными темами. Поскольку потребность в образовании становится более очевидной.

Многие практики информационной безопасности и конфиденциальности на протяжении многих лет высказываются о нехватке образованных кадров, а полученное образование в ВУЗах в большинстве своем далеко от практики или лишено конкретных практических навыков. Такая ситуация вызвана многими факторами, но основным является не упадок высшего образования, а потребность практиков не в выпускниках с высшим образованием, а в специалистах со среднетехническим образованием, именно этот пласт образования наиболее пострадал в реформах последних десятилетий.

Создание среднего профессионального образования – это трудоемкий и длительный процесс с учетом того, что: первое – это изменилось мировоззрение людей к среднему профессиональному образованию, т.к. все хотят иметь высшее образование, несмотря ни на что; второе – практически полностью утрачен статус этой формы образования и самое главное его

уклад и инфраструктура, производственные учебные комплексы и комбинаты.

Развиваемое в настоящее время среднее образование строится на базе ВУЗов, что на мой взгляд выглядит несколько дискредитирующим моментом отпугивая от этой формы потенциальных обучаемых. Поэтому основным путем устранения нехватки образования при решении служебных задач является повышение квалификации или просто занятия по информированию сотрудников без выписки удостоверений и дипломов о полученном обучении.

Информирование может производиться различными приемами. Могут организовываться семинары и конференции, курсы по осведомленности, информационная рассылка в корпоративной сети, информационные буклеты, а также контролирующие качество подготовки экзамены, тесты и опросы.

Стоит отметить большой недостаток методологии и исследований по обучению взрослых информационной безопасности. Образование должно основываться на надежных исследованиях в области обучения взрослых и включаться в образовательную программу для практиков информационной безопасности и конфиденциальности. Образование должно быть адаптировано к потребностям организации и целевых учащихся.

С течением времени все больше и больше происходит инцидентов информационной безопасности и нарушений конфиденциальности, и даже многие образованные специалисты могут заблуждаться в своих познаниях из-за стремительного развития информатизации и программного обеспечения, что сказывается на принятии не правильных решений, что уж тут говорить о людях лишенных даже первичных знаний о информационной безопасности.

Почти в каждом инциденте информационной безопасности и нарушении конфиденциальности люди были в конечном счете причиной, иногда из-за злого умысла, но чаще из-за отсутствия знаний и осведомленности или допущенных ошибок, или упущений, часто потому, что безопасность и конфиденциальность не были очевидным элементом работы с вычислительными системами. Даже когда речь идет о злонамеренных поступках, они, как правило, каким-то образом используют неосведомленность о информационной безопасности человека.

Компьютерные системы и приложения должны быть построены с более надежными и более прозрачными возможностями безопасности, чем в настоящее время. Однако нельзя создать компьютерную технологию, настолько безопасную, чтобы не требовалось обучение пользователей компьютеров. Это все равно, что сказать, что вы можете построить автомобиль настолько безопасным, что вам не нужно учить людей, как безопасно ездить. И, во всяком случае, когда дело доходит до эффективной информационной безопасности и защиты конфиденциальности, эффективная и регулярная информационная безопасность, обучение конфиденциальности и постоянные информационные коммуникации абсолютно необходимы на всех уровнях предприятия. Системы и приложения не будут построены с этими гарантиями без обучения тех, кто их строит.

Не только ум и мудрость руководителей, определяет важность регулярного

обучения и постоянную информационно-разъяснительную работу, для предотвращения инцидентов информационной безопасности и нарушения конфиденциальности, но также эти требования отражены в большинстве законов и правил о защите данных. Это одно из важнейших понятий, которое признали руководители практически всех развитых стран мира. Потребность обучения информационной безопасности нашло отражение в многочисленных законах, постановлениях и регламентах.

Одним из наиболее экономически эффективных и результативных методов обеспечения эффективной информационной безопасности и конфиденциальности, направленной на сохранение своих информационных и финансовых активов в безопасности, является тотальное обучение и повышение осведомленности всех сотрудников предприятия.

Руководители бизнеса должны понимать, что, если поставщики технологий говоря вам, о пустой трате времени на обучение, скорее всего, намерены положить руки в ваши карманы, для получения гораздо большей прибыли, чем любые инвестиции в образование, чтобы продать вам систему или приложение, которое в десять – сотни раз превышает стоимость любой образовательной программы, которую вы могли бы создать сами и проводить опережающее обучение.

Успех любой программы повышения осведомленности и обучения зависит от использования продуманного, систематического подхода для обеспечения эффективной деятельности по повышению осведомленности и учебных занятий для вашей целевой аудитории. Эффективность обучения может быть достигнута в результате творческого подхода к выбору разнообразных методов и приемов, которые практикующие специалисты должны адаптировать каждый раз к обучаемой аудитории для получения максимальной положительной ответной реакции.

Библиографический список

1. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895).
2. Белов, Е.Б. Состояние, проблемы и развитие профессионального образования в области информационной безопасности / Е.Б. Белов // Безопасность информационных технологий. – 2005. – №1. – С. 6-13.
3. Белов, Е.Б., Лось, В.П. Образование в области информационной безопасности: принципы совершенствования подготовки кадров / Е.Б. Белов, В.П. Лось // Информация и связь. – 2002. – №2. – С. 94-96.
4. Военная дидактика: Учебник / Под общ. ред. В.Г. Михайловского. – М.: МО РФ, 2005.
5. Курко, И.Н. Методическая система открытого обучения дисциплине "Программно-аппаратные средства обеспечения информационной безопасности": Дис. ...канд. пед. наук: 13.00.02. – Красноярск. – 2004. – 158 с.
6. United States Sentencing Commission, Sentencing Guidelines for United States Courts, http://www.ussc.gov/FEDREG/05_04_notice.pdf.
7. Robert L. Craig. The history of training, in The ASTD Training and Development Handbook, 4th edition, McGraw-Hill, New York, 1996, p. 4.

EDUCATIONAL NEEDS FOR INFORMATION SECURITY

B.A. Shvyrev, *candidate of physical and mathematical sciences, leading researcher*
Research institute of the federal penitentiary service of Russia
 (Russia, Moscow)

***Abstract.** The relevance of education in the direction of "Information Security" is considered. The need for specialists with secondary technical education is revealed. Defined pedagogical approaches to replenish the knowledge of practitioners. The importance of continuing education in matters of information security is noted. The effectiveness of information security training can be achieved as a result of a creative approach to choosing a variety of methods and techniques that practitioners must adapt each time to the trained audience in order to obtain the maximum positive response.*

***Keywords:** information security training, continuous education, outreach.*