УДК 004

ВЫБОР СЕРТИФИЦИРОВАННЫХ ПРОГРАММНЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ЭФФЕКТИВНОЙ ИХ РАБОТЫ НА ПРЕДПРИЯТИИ

М.С. Говоров[1], М.И. Данилов[2]

1 *mikhail_gavorov_181@mail.ru*; Казанский национальный исследовательский технический университет им. А.Н. Туполева

2 *maksim_ivanovich_d@mail.ru*; Казанский национальный исследовательский технический университет им. А.Н. Туполева

В статье предложен подход выбора программных и технических средств информационной защиты, обоснована необходимость прохождения государственной сертификации для решения задачи эффективного обеспечения защиты информации на предприятии.

Ключевые слова: защита информации, объект информатизации, сертификация средств защиты информации.

Очевидно, что для максимально эффективной защиты информации рекомендуется использовать только соответствующие определенным требованиям (государственным стандартам) средства ее обработки. Для защиты от недоброкачественной продукции все средства обработки информации и ее защиты, согласно закону № 149-ФЗ от 27.07.2006г. «Об информации, информационных технологиях и о защите информации», должны проходить обязательную государственную сертификацию. Наличие сертифицированных средств дает преимущества при проведении страхования информации.

Стоит упомянуть, что сертифицируются защищенные технические, программно-технические, программные средства, системы, сети вычислительной техники и связи, средства защиты и средства контроля эффективности защиты. При этом если в работе используется информация с ограниченным доступом или составляющая государственную тайну, то средства, в том числе и иностранного производства, должны пройти обязательную сертификацию. В остальных случаях сертификация носит добровольный характер. Сертификацию проводят специальные службы: ФСБ – для средств защиты информации, использующих методы криптографии и шифрования; и ФСТЭК — для средств защиты информации, не использующих таких методов. Приведенные службы уполномочены предъявлять требования, обеспечивающие нужную степень защиты, и выступают государственным гарантом строгого их выполнения. Также в целях обеспечения лучшей защиты и минимизации последующих затрат стоит убедиться в наличии сертификата качества от РОССТАНДАРТ.

В России создана система сертификации средств защиты по требованиям безопасности информации. Многие производители, понимая преимущества сертифицированного продукта на рынке, подают заявки на испытания. На данный период многие хорошие программные и технические средства прошли сертификацию. В их числе есть и специальные программы, обеспечивающие защиту от несанкционированного доступа, и защищенные технические средства зарубежных и отече-

ственных производителей, и специальные средства защиты от побочных электромагнитных излучений и наводок, и многое другое.

Перечни средств защиты, прошедших сертификацию с указанием производителей и их адресов, постоянно обновляются и рассылаются ФСТЭК во все администрации регионов и заинтересованные министерства. Есть эта информация и в Госстандарте России, который ведет общий перечень средств, имеющих различные сертификаты, а также у всех лицензиатов, которые выполняют работы по защите. Кроме того, всегда можно обратиться непосредственно в ФСТЭК России или его филиалы и получить квалифицированную консультацию [1-7].

Что касательно средств, не имеющих соответствующего сертификата, то выставить продукцию на сертификацию может не только производитель, но и потребитель. Для этого следует подготовить по специальной форме заявку в федеральный орган по сертификации, после ее рассмотрения будет назначена одна из испытательных лабораторий, аккредитованная в Системе сертификации, а далее – испытания, отчет, рассмотрение результатов экспертной комиссией и (при положительных результатах) получение сертификата от федерального органа по сертификации. Правда, в этом случае выдается единичный сертификат на каждый конкретный образец продукции, поэтому и стоить эта процедура будет дороже. Но иногда, особенно если вы в своей работе используете уникальный программный или технический продукт, без которого нельзя обойтись, эти расходы будут оправданы.

Выбирайте средства защиты из уже прошедших сертификацию. Но если требуется сертифицировать новые средства, то не обращайтесь по этому вопросу сразу в известную испытательную лабораторию – это сэкономит время, потому как решение о назначении для проведения сертификации той или иной испытательной лаборатории все равно принимается органом по сертификации ФСТЭК России, и не всегда оно будет совпадать с вашими желаниями.

Литература

1. Петровский В.И. Оптимизация комплексной системы защиты информации на предприятиях различных форм собственности / В.И. Петровский, М.В. Тумбинская, М.В. Петровский // Вестник НЦБЖД. – 2016. – № 3 (29). – С. 94–102.

2. Petrovsky V. The history and prospects of information security at russian enterprises / V. Petrovsky, M. Tumbinskaya // 3rd International Conference on Computer Technology in Russia and in the Former Soviet Union: proceedings of conference. – Kazan, 2015. – P. 143–146.

3. Трегубов В.М. Оптимизация построения службы КСЗИ и ПДТРЗ в государственном образовательном учреждении как объекте информатизации / В.М. Трегубов // Поиск эффективных решений в процессе создания и реализации научных разработок в российской авиационной и ракетно-космической промышленности: материалы международной научно-практической конференции. – Казань, 2014. – С. 556–563.

4. Сафиуллина А.М. Программное обеспечение оценивания тестовых заданий для выявления компетенций кадрового резерва с элементами защиты информации / А.М. Сафиуллина // Национальные интересы: приоритеты и безопасность. – 2012. – № 35. – С. 42–47.

SELECTION OF CERTIFIED INFORMATION PROTECTION SOFTWARE AND TECHNICAL SECURITY PRODUCTS TO ENSURE THEIR EFFECTIVE OPERATION AT THE ENTERPRISE

M.S. Govorov, M.I. Danilov

The article proposes an approach to the selection of software and technical products of information protection, substantiates the need for passing state certification to get the most effective information protection at the enterprise.

Keywords: information protection, certification of information protection software, technical security product.

УДК 372.851

О РОЛИ ТЕХНОЛОГИЧЕСКОГО ПОДХОДА

А.Н. Гузялова[1]

1 *alina_guzyalova@mail.ru*; Казанский (Приволжский) федеральный университет

В данной статье приводится краткая история становления технологического подхода к обучению, рассматриваются уровни и особенности технологии.

Ключевые слова: технология, технологический подход, программированное обучение, педагогическая технология.

Все пойдет вперед не менее ясно, чем идут часы с правильно уравновешенными тяжестями, так же приятно и радостно, как приятно и радостно смотреть на такого рода автомат, и, наконец с такой верностью, какую только можно достигнуть в подобном искусном инструменте.
Я.А.Коменский

Ян Амос Коменский старался отыскать всеобщий порядок преподавания. Он полагал, что все можно было бы “преподавать единообразно”, чтобы обучение шло вперед “не менее ясно, чем идут часы” [2]. С тех пор в педагогике усилия отыскать свершенный метод не прекращалась. Однако человечество не приблизилось к идеалу сбалансированного учебного процесса. И это вовсе не от бессилия науки…

В последнее 20 лет исследования в области ТСО (технические средства обучения) устремлены на переход к применению в учебном процессе новых информационных технологий, прежде всего компьютеров. Такое направление называется “технологии в обучении”.

Руководитель образовательного направления “Организации экономического сотрудничества и развития” говорит: “Технология может усилить хорошее обучение, но не сможет компенсировать плохое обучение”. Что означает понятие “педагогическая технология”? Еще совсем недавно педагогическая наука и практика обходилась без этого понятия. Однако, по мнению современных педагогов, приход “технологии” был предрешен, потому что развитие и потребности образования требовало это на современном этапе развития.

Понятие “технология” имеет определенную историю своего становления в педагогической науке. В США, а позднее в Западной Европе, были первые попытки