УДК 004.056.53

ПОВЫШЕНИЕ КАЧЕСТВА УПРАВЛЕНИЯ ОБРАЗОВАТЕЛЬНЫМ УЧРЕЖДЕНИЕМ ПУТЕМ ВНЕДРЕНИЯ В УЧЕБНЫЙ ПРОЦЕСС СОВРЕМЕННЫХ ИНФОРМАЦИОННО БЕЗОПАСНЫХ СРЕДСТВ

Е.И. КАШИРИНА, А.С. ПОЛИКАРЕНКОВ

Кубанский государственный технологический университет,
350002, Российская Федерация, г. Краснодар, ул. Московская, 2;
электронная почта: 11figura11@mail.ru

В современном обществе уделяется много внимания информационной безопасности банков, предприятий, государственных структур и других объектов. Безопасность информации, обрабатываемой в школе, остается на низком уровне. Большое внедрение современной компьютерной техники, широкополосный доступ в интернет, а также низкая квалификация или отсутствие системных администраторов делает школу все более привлекательной для атак злоумышленников. В погоне за качеством образования теряется безопасность, как немаловажная составляющая. Для исправления данной ситуации была предложена типовая «модель нарушителя» и «модель угроз» для средней школы. Исходя из составленной «модели угроз», предложено примерное оборудование для реализации, а также дано обоснование.

Ключевые слова: модель угроз, модель нарушителя, персональные данные, антивирус, межсетевой экран, интернет вещей.

Трансформация экономической среды России, связанная с изменением, прежде всего, социально-политической системы, а также с изменениями мирового хозяйства в условиях глобализации, сопровождается значительным усилением роли экономической безопасности в частности образовательных учреждений, как фундаментальной основы экономически эффективного государства [5, 6]. Мировой финансовый кризис предопределил необходимость формирования в нашем государстве отлаженной системы экономической безопасности, обеспечивающей развитие экономики законными и эффективными методами.

Одной из важнейших характеристик работы экономической системы является обеспечение эффективного функционирования деятельности как предприятий сферы реального сектора, так и организаций, учреждений сферы услуг. В исследовании предлагается обратить внимание на образовательные учреждения [1, 2]. Для этого необходимо осуществить прогноз возможных факторов риска, опасностей и угроз экономической безопасности, а также принять экстренные меры для того, чтобы не допустить или ослабить их возникновение. В

статье рассматриваются основные угрозы экономической безопасности, раскрывается их содержание и характер влияния в рамках построения системы обеспечения экономической безопасности образовательного учреждения. Основной задачей такого учреждения является донесение до слушателя достоверной, актуальной и цельной информации. С целью достижения наиболее высокого уровня восприятия слушателем информации, необходимо внедрение новых технологий обучения [3].

Век информационных технологий несет в себе глобальную информатизацию общества [7, 8]. Во всех отраслях наблюдается переход от бумажных носителей к компьютерам. Такую тенденцию можно проследить на примере школ. Высокоскоростной доступ в интернет организован в каждой школе, школьные журналы посещаемости и оценок заменяются на электронные, внедряются электронные доски и учебники, а также другие современные технологии. Качество образования стремится вверх за счет внедрения инновационных технологий. Но так ли безобидны современные средства информатизации? Только ли пользу они несут?

Современные технологии обучения в школах почти не рассматриваются с точки зрения информационной защищенности, а между тем, в них обрабатываются личные персональные данные каждого из обучающихся, их родителей и учителей, широкополосный доступ в интернет и большое количество компьютеров и устройств IoT («Интернет вещей») в сети могут состоять в ботнет-сети, и совершать атаки типа «отказ в обслуживании» по всему миру. Это только несколько из возможных сценариев действий злоумышленников. Недостаточное внимание к безопасности устройств, имеющих выход в интернет, низкий уровень защищенности сети, а также низкая квалификация или полное отсутствие системного администратора делает привлекательными для злоумышленников образовательные учреждения.

Проблема становится актуальной на сегодняшний день, поскольку наблюдается ежегодный рост кибератак на государственные учреждения, основная задача которых – снижение качества оказываемых услуг и доверия к госу-

дарственному органу со стороны населения. Для решения этого вопроса необходим единый комплексный подход, который должен содержать в себе анализ возможного нарушителя, его действий, а также контрмеры, которые мы должны принять для предотвращения атаки или минимизации потенциального ущерба [4].

Угроза качеству образования возникла из-за внесистемного подхода к информатизации учебных заведений. До сих пор нет официально прописанного регламента работ по информатизации школ, нет единого координационного центра, а также общего представления о «современной» школе. Каждое учебное заведение решает данный вопрос самостоятельно, опираясь на собственный опыт и опыт коллег, что не всегда является верным решением. И если при покупке современной техники в общеобразовательное учреждение директор может самостоятельно определить перечень необходимого оборудования, то при покупке современных систем информационной безопасности мало у кого получится сделать правильный выбор.

Невозможно построить защищенную систему без четкого понимания двух вопросов: Кто может нарушить работу системы и каким образом? Данная задача должна быть индивидуальна для каждой школы в отдельности, но в силу одного профиля заведений и примерно равных условий работы: защищенный периметр школы, компьютерные классы, оборудованные компьютерами, из расчета один компьютер на двух учеников, и индивидуальный компьютер на рабочем столе каждого учителя, составим типовые модель нарушителя и модель угроз.

Опишем модель нарушителя в таблице 1.

Таблица 1 – Модель нарушителя

№ п/п	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности
1	Внешние субъекты (физические лица)	Внешний	Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Причинение имущественного ущерба путем мошенничества или иным преступным путем Проверка (тестирование) своих возможностей

Окончание таблицы 1

2	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	Непреднамеренные, неосторожные или неквалифицированные действия
3	Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру операторы (администрация, охрана, уборщики и т.д.)	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием Непреднамеренные, неосторожные или неквалифицированные действия Любопытство Причинение имущественного ущерба путем мошенничества или иным преступным путем
4	Пользователи информационной системы (учителя)	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием Причинение имущественного ущерба путем мошенничества или иным преступным путем Непреднамеренные, неосторожные или неквалифицированные действия Месть за ранее совершенные действия
5	Администраторы информационной системы	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием Причинение имущественного ущерба путем мошенничества или иным преступным путем Любопытство или желание самореализации (подтверждение статуса) Непреднамеренные, неосторожные или неквалифицированные действия Месть за ранее совершенные действия
6	Пользователи информационной системы (ученики учебного заведения)	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием Любопытство или желание самореализации (подтверждение статуса) Непреднамеренные, неосторожные или неквалифицированные действия Месть за ранее совершенные действия
7	Бывшие работники (пользователи)	Внешний	Месть за ранее совершенные действия Причинение имущественного ущерба путем мошенничества или иным преступным путем

Исходя из данных, приведенных в модели нарушителя безопасности, составление модели угроз безопасности может быть описано следующим образом. Типы нарушителей бывают двух видов внутренние и внешние. В зависимости от вида нарушителей и их целей существует целый ряд мотивов или возможных целей реализации угроз безопасности. Основными являются некомпе-

тентность, причинение имущественного ущерба и как не странно, но любопытство. Далее рассмотрим модели угроз безопасности в таблице 2.

Таблица 2 – Модель угроз безопасности

№ п/п	Наименование угрозы	Вероятность реализации угрозы	Опасность угрозы	Актуальность угрозы	Меры противодействия угрозе	
					Технические	Организационные
1	Кража ПЭВМ	Маловероятна	Низкая	Неактуальная	-	Пропускной режим Охрана Регулярная инвентаризация
2	Кража носителей информации	Маловероятна	Средняя	Актуальная	-	Пропускной режим Охрана
3	Кража, модификация, уничтожение информации	Высокая вероятность	Низкая	Актуальная	-	
4	Вывод из строя узлов ПЭВМ, каналов связи	Маловероятна	Низкая	Неактуальная	-	Пропускной режим Охрана
5	Несанкционированное отключение средств защиты	Низкая вероятность	Низкая	Неактуальная	Настройка средств защиты	Инструкция системного администратора
6	Действия вредоносных программ (вирусов)	Средняя вероятность	Низкая	Актуальная	Антивирусное ПО «Касперский 6.0»	Инструкция пользователя
7	Установка ПО не связанная с исполнением должностных обязанностей	Средняя вероятность	Низкая	Актуальная	-	Инструкция пользователя Инструкция ответственного
8	Утрата ключей и атрибутов доступа	Средняя вероятность	Низкая	Неактуальная	-	Инструкция пользователя Инструкция системного администратора
9	Непреднамеренная модификация (уничтожение) информации сотрудниками	Высокая вероятность	Средняя	Актуальная	Настройка средств защиты	Инструкция пользователя
10	Выход из строя аппаратно-программных средств	Средняя вероятность	Низкая	Неактуальная	-	-
11	Сбой системы энергоснабжения	Маловероятна	Низкая	Неактуальная	Использование источника бесперебойного питания	-

Окончание таблицы 2

12	Стихийное бедствие	Маловероятна	Низкая	Неактуальная	Пожарная сигнализация	Инструкция по действиям в случае возникновения нештатной ситуации
13	Доступ к информации, модификация, уничтожение лицами не допущенными к её обработке	Средняя вероятность	Низкая	Актуальная	-	-
14	Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	Низкая вероятность	Средняя	Актуальная	-	-
15	Угрозы выявления паролей по сети	Маловероятна	Низкая	Неактуальная	-	-
16	Угрозы навязывания ложного маршрута сети	Маловероятна	Низкая	Неактуальная	-	-
17	Угрозы подмены доверенного объекта в сети	Маловероятна	Низкая	Неактуальная	-	-
18	Угрозы типа «Отказ в обслуживании»	Маловероятно	Низкая	Неактуальная	-	-
19	Угрозы удаленного запуска приложений	Маловероятно	Низкая	Неактальная	-	-
20	Угрозы внедрения по сети или локально вредоносных программ	Низкая вероятность	Средняя	Актуальная	Антивирусное ПО «Касперский 6.0»	-

Используя полученные данные, можно сделать вывод, что для обеспечения безопасности персональных данных, обрабатываемых в школах, а также безопасного использования доступа в интернет, необходимо принятие мер по защите информации, в частности, обновление антивируса до более новой версии (Антивирус Kaspersky 10.0), а также грамотная его настройка, контроль и

ограничение доступа подключения к сетям Wi-Fi, установка шифрованного, VPN канала передачи данных, между школой и министерством образования (ViPNet), использование электронной подписи при передачи документов (CryptoPro) а также установка межсетевого экрана на сайт школы(WAF).

Предложенные в статье меры являются необходимыми, но не достаточными. Достаточной мерой будет являться присутствие в штате школы должности «Специалист по информационной безопасности», который сможет оперативно реагировать на инциденты информационной безопасность, редактировать политики безопасности, производить своевременные аудиты безопасности и обновления.

Качество оказания услуг – одна из приоритетных задач нашего государства и министерства образования, в частности. Немаловажной частью оказания услуги является неразглашение конфиденциальных данных, в том числе и при обучении ребенка в школе. К сожалению, анализ статистики подтверждает, что с каждым годом количество киберпреступлений только растет, и злоумышленники расширяют спектр своих атак. Необходимо уже сейчас начать заботиться о безопасности объектов информатизации, ведь это позволит защитить созданные технологии, методики и другие научные изыскания, а также защитит от несанкционированного доступа к имеющемуся высокотехнологичному оборудованию.

Работа выполнена в рамках I Научно-методической конференции, посвященной всемирному дню качества: «Стратегия качества в эффективном менеджменте: опыт построения системы менеджмента качества», КубГТУ, 10 ноября 2016.

ЛИТЕРАТУРА

1. Третьяков П.И. Практика управления современной школой. – М.: Новая школа, 2015. – 200 с.

2. Панферова Н.Н. Управление в системе образования. − Ростов-на-Дону: Феникс, 2010. − 248 с.

3. Попова Г.П., Размерова Г.А., Ремчукова И.Б. Мониторинг качества учебного процесса: принципы, анализ, планирование – Волгоград: Учитель, 2012. – 124 с.

4. Ярных В.И. Качество образования как один из ключевых факторов международной конкуренции в системе образования // Вестник РГГУ. Серия: История. Филология. Культурология. Востоковедение. 2016. № 4 (13). С. 96-104.

5. Ермоленко Н.Ю., Ермоленко А.А. Интеллектуальный капитал высшего образования // Вестник Адыгейского государственного университета. Серия 5: Экономика. – 2014. - № 4. – С. 15-19.

6. Захарова Е.Н., Полинко А.В. Эволюция подходов к использованию информационных технологий в бизнес-деятельности / Приоритеты и механизмы обеспечения экономического роста, финансовой стабильности и социальной сбалансированности в России. Сборник статей. – 2016. С. 45-49.

7. Клочко Е.Н., Межлумова В.Р., Бугаенко В.Э. Структурно-функциональное моделирование развития научно-исследовательской деятельности студентов в высшей школе // Представительная власть - XXI век: законодательство, комментарии, проблемы. -2016. - № 4 (147). - С. 37-41.

8. Клочко Е.Н., Межлумова В.Р. Раскрытие принципов оптимизации взаимодействия научного и образовательного процессов в условиях модернизации сферы образовательных услуг РФ // Вестник Адыгейского государственного университета. Серия «Экономика». – Майкоп: издательство АГУ, 2015. – № 1 (155). – 245 с. – С. 189-195

REFERENCES

1. Tretyakov P.I. Praktika upravleniya sovremennoy shkoloy. – M.: Novaya shkola, 2015. – 200 s.

2. Panferova N.N. Upravlenie v sisteme obrazovaniya. − Rostov-na-Donu: Feniks, 2010. − 248 s.

3. Popova G.P., Razmerova G.A., Remchukova I.B. Monitoring kachestva uchebnogo protsessa: printsipy, analiz, planirovanie – Volgograd: Uchitel, 2012. – 124 s.

4. Yarnykh V.I. Kachestvo obrazovaniya kak odin iz klyuchevykh faktorov mezh-dunarodnoy konkurentsii v sisteme obrazovaniya // Vestnik RGGU. Seriya: Isto-riya. Filologiya. Kulturologiya. Vostokovedenie. 2016. № 4 (13). S. 96-104.

5. Ermolenko N.Yu., Ermolenko A.A. Intellektualnyy kapital vysshego obrazovaniya // Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 5: Ekonomika. – 2014. - № 4. – S. 15-19.

6. Zakharova E.N., Polinko A.V. Evolyutsiya podkhodov k ispolzovaniyu informatsionnykh tekhnologiy v biznes-deyatelnosti / Prioritety i mekhanizmy obespecheniya ekonomicheskogo rosta, finansovoy stabilnosti i sotsialnoy sbalansirovannosti v Rossii. Sbornik statey. – 2016. S. 45-49.

7. Klochko E.N., Mezhlumova V.R., Bugaenko V.E. Strukturno-funktsionalnoe modelirovanie razvitiya nauchno-issledovatelskoy deyatel-nosti studentov v vysshey shkole // Predstavitelnaya vlast - XXI vek: zakono-datelstvo, kommentarii, problemy. -2016. - № 4 (147). - S. 37-41.

8. Klochko E.N., Mezhlumova V.R. Raskrytie printsipov optimizatsii vzaimodeystviya nauchnogo i obrazovatelnogo protsessov v usloviyakh modernizatsii sfery obrazovatelnykh uslug RF // Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya «Ekonomika». – Maykop: izdatelstvo AGU, 2015. – № 1 (155). – 245 s. – S. 189-195

IMPROVEMENT OF QUALITY OF MANAGEMENT OF EDUCATIONAL ESTABLISHMENT BY INTRODUCTION IN EDUCATIONAL PROCESS OF MODERN IT IS INFORMATION SAFE MEANS

E.I. KASHIRINA, A.S. POLIKARENKOV

Kuban State Technological University,
2, Moskovskaya St., Krasnodar, Russian Federation, 350002,
e-mail: 11figura11@mail.ru

In modern society, much attention is paid to information security of banks, businesses, government structures and other objects. Security of information processed in the school, remains at a low level. Great integration of modern computer technology, broadband Internet access, and also low qualification or lack of system administrators makes the school more attractive to attackers. In pursuit of quality education is lost security as an important component. To remedy this situation were proposed and a model "model of the intruder" and "threat model" for middle school. On the basis of made up "threat model" offered exemplary hardware to implement, and also the substantiation.

Key words: threat model, the model of the intruder, the personal data, antivirus, firewall, Internet of things