АНАЛИЗ СУЩЕСТВУЮЩИХ МОДЕЛЕЙ И МЕТОДОВ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.К. Курманбай, студенка гр. 17В41
Научный руководитель: Разумников С.В.
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E–mail:aigera_0796@mail.ru

В настоящее существуют различные методики, предназначенные для оценки рисков и информационной безопасности ИС. Рассмотри некоторые из них.

Метод CRAMM (CCTA Risk Analysis and Managment Method) был разработан Агентством по компьютерам и телекоммуникациям Великобритании (Central Computer and Telecommunications Agency) по заданию Британского правительства и взят на вооружение в качестве государственного стандарта. Он используется, начиная с 1985 г., правительственными и коммерческими организациями Великобритании. За это время CRAMM приобрел популярность во всем мире. Фирма Insight Consulting Limited занимается разработкой и сопровождением одноименного программного продукта, реализующего метод CRAMM.

К недостаткам метода CRAMM можно отнести следующее: использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора; CRAMM в гораздо большей степени подходит для аудита уже существующих ИС, находящихся на стадии эксплуатации, нежели чем для ИС, находящихся на стадии разработки; аудит по методу CRAMM – процесс достаточно трудоемкий и может потребовать месяцев непрерывной работы аудитора; программный инструментарий CRAMM генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике; CRAMM не позволяет создавать собственные шаблоны отчетов или модифицировать имеющиеся; возможность внесения дополнений в базу знаний CRAMM не доступна пользователям, что вызывает определенные трудности при адаптации этого метода к потребностям конкретной организации; программное обеспечение CRAMM существует только на английском языке; стоимость лицензии от 2000 до 5000 долл.

Программное обеспечение RiskWatch является мощным средством анализа и управления рисками. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности. Оно включает в себя следующие средства аудита и анализа рисков[4]:

RiskWatch for Physical Security – для физических методов защиты ИС;

RiskWatch for Information Systems – для информационных рисков;

HIPAA–WATCH for Healthcare Industry – для оценки соответствия требованиям стандарта HIPAA (US Healthcare Insurance Portability and Accountability Act); RiskWatch RW17799 for ISO 17799 – для оценки требованиям стандарта ISO 17799.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются предсказание годовых потерь (Annual Loss Expectancy, ALE) и оценка возврата от инвестиций (Return on Investment, ROI).

К недостаткам RiskWatch можно отнести: Такой метод подходит, если требуется провести анализ рисков на программно–техническом уровне защиты, без учета организационных и административных факторов[5]. Полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывает понимание риска с системных позиций – метод не учитывает комплексный подход к информационной безопасности. Программное обеспечение RiskWatch существует только на английском языке. Высокая стоимость лицензии (от 10 000 долл. за одно рабочее место для небольшой компании) [7].

ГРИФ – комплексная система анализа и управления рисками информационной системы компании. ГРИФ 2006 из состава Digital Security Office дает полную картину защищенности информационных ресурсов в системе и позволяет выбрать оптимальную стратегию защиты информации компании.

Система ГРИФ: Анализирует уровень защищенности всех ценных ресурсов компании; оценивает возможный ущерб, который понесет компания в результате реализации угроз информационной безопасности; позволяет эффективно управлять рисками при помощи выбора контрмер, наиболее оптимальных по соотношению цена/качество

Метод OCTAVE – это трехэтапный подход оценки рисков информационной безопасности. На первой стадии осуществляется оценка организационных аспектов. Во время выполнения этой стадии ГА определяет критерии (показатели) оценки ущерба (неблагоприятных последствий), которые поз-

же будут использоваться при оценке рисков. Здесь же осуществляется определение наиболее важных организационных ресурсов и оценка текущего состояния практики обеспечения безопасности в организации. На завершающем этапе первой стадии определяются требования безопасности, и строится профиль угроз для каждого критического ресурса.

На второй стадии проводится высокоуровневый анализ ИТ –инфраструктуры организации, при этом обращается внимание на степень, с которой вопросы безопасности решаются и поддерживаются подразделениями и сотрудниками, отвечающими за эксплуатацию инфраструктуры. На третьей стадии проводится разработка стратегии обеспечения безопасности и плана защиты информации [5].

Этот этап складывается из определения и анализа рисков и разработки стратегии обеспечения безопасности и плана сокращения рисков. В процессе определения и анализа рисков оценивают ущерб от реализации угроз, устанавливают вероятностные критерии оценки угроз, оценивают вероятность реализации угроз. В процессе разработки стратегии обеспечения безопасности и плана сокращения рисков: • описывают текущую стратегию безопасности, выбирают подходы сокращения рисков, разрабатывают план сокращения рисков, определяют изменения в стратегии обеспечения безопасности, определяют перспективные направления обеспечения безопасности. В целом из приведенного анализа можно сделать вывод, что методы и системы имеют свой плюсы и минусы,

Литература

1. Официальный сайт www.riskwatch.com Электронный ресурс: Режим доступа http://www.riskwatch.com/ Дата обращения: 10.05.2016г.
2. Разумников С.В. Анализ возможности применения методов Octave, RiskWatch, Cramm для оценки рисков ИТ для облачных сервисов //Современные проблемы науки и образования. -2014 -№ 1. -С. 1. -Режим доступа: http://www.science-education.ru/115-12197.
3. ГОСТ Р 55368 – 2012/ ISO/IEC Guide 28:2004 Оценка соответствия. Методические указания по системе сертификации продукции третьей стороной.
4. Разумников С.В., Фисоченко О.Н., Лунегов В.Ю. Информационная система оценки возможности корпоративных ИТ-приложений для миграции в облачную среду [Электронный ресурс] // Современные проблемы науки и образования. - 2014 - №. 4. - С. 1. - Режим доступа: http://www.science-education.ru/118-13924.
5. Разумников С.В. Использование метода линейного программирования для оценки эффективности применения облачных ИТ-сервисов // Приволжский научный вестник. - 2013- №. 7(23). - С. 43-45.

ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ФИЗИЧЕСКОЙ КУЛЬТУРЫ И СПОРТА

А.К. Курманбай, студенка гр. 17В41
Научный руководитель: Счастливцева И. В.
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E–mail:aigera_0796@mail.ru

Качественное и своевременное обеспечение документами и информацией преподавателей, студентов, спортсменов, тренеров, всех людей занимающихся и интересующимися спортом является одним из важнейших факторов реализации и развития спорта. Для студентов ЮТИ ТПУ это в первую очередь развитие спорта и спортивной активности в институте и регионе.

В данной работе рассматриваются проблемы информационного обеспечения физической культуры и спорта, которая в последнее время одним из актуальных направлений исследований, особенно за рубежом.

Информационные потребности и особенности поведения студентов при самостоятельном поиске информации в связи с появлением новых возможностей информационных потребностей посредством доступа к электронным информационным ресурсам через глобальные телекоммуникационные сети, то есть интернет, который существенно меняют сложившиеся представления о понятии документа, информации и методике информационного поиска.

Проблема современного информационного обеспечения институтов остается мало изученной. Кроме того, уровень информационного обеспечения физической культуры и спорта на школьных, институтских уровнях, особенно на периферии, остается невыясненным.