

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

УДК 378.14:004.7.056
ББК [32.973-018.2:32.81]р30-2

С. В. Белов, А. Х. Нурзбаева

МЕТОДИКА ОБУЧЕНИЯ СТУДЕНТОВ НАВЫКАМ ПРОВЕДЕНИЯ ОБСЛЕДОВАНИЯ ОБЪЕКТА ЗАЩИТЫ ИНФОРМАЦИИ

S. V. Belov, A. Kh. Naurzbaeva

TECHNIQUE OF TRAINING OF STUDENTS TO SKILLS OF CARRYING OUT INSPECTION OF AN OBJECT OF INFORMATION SECURITY

Рассматриваются вопросы разработки контрольных заданий по информационной безопасности с использованием механизмов деловой игры. Проведен системный анализ объекта защиты информации в соответствии с требованиями нормативных документов в области информационной безопасности. Выявлены основные характеристики объекта защиты, необходимые для проведения его предварительного обследования с использованием методов опроса, просмотра его информационных и физических параметров. Предложена методика, позволяющая оценить умение сбора информации об информационных ресурсах, ее анализа и выявления возможных угроз безопасности информации для дальнейшего построения системы информационной безопасности, включающего разработку организационно-технической документации.

Ключевые слова: объект защиты информации, информационная безопасность, проектирование систем информационной безопасности.

The questions of development of control tasks on information security with the use of mechanisms of business game are considered. The system analysis of an object of information security according to the requirements of normative documents in the field of information security is carried out. The main characteristics of an object of the protection necessary for carrying out its preliminary survey with the use of methods of poll, viewing of its information and physical parameters are revealed. The technique allowing estimation of the ability to collect information about information resources, its analysis and identification of possible threats of safety of information for further creation of the system of the information security, including the development of organizational technical documentation, is offered.

Key words: object of information security, information security, projection of systems of information security.

Введение

Развитие отрасли информационной безопасности (ИБ) приводит к возрастанию спроса на специалистов по защите информации, обладающих высокой информационной культурой, владеющих новейшими информационными технологиями и умеющих применять в своей профессиональной деятельности приобретенные знания и навыки. Подготовка специалистов в области ИБ, обучение их способам построения комплексных систем защиты информации, применения аппаратно-программных средств защиты становятся приоритетными условиями поддержания нормального функционирования как коммерческих, так и государственных структур.

Согласно федеральным государственным образовательным стандартам третьего поколения, в учебном процессе необходимо использовать активные и интерактивные формы проведения занятий.

Методы обучения должны выбираться с учетом содержания учебного материала и целей обучения, которые предполагают не только приобретение знаний, но и формирование умений и навыков, необходимых в практической работе. Именно поэтому в учебном процессе необходимы в первую очередь те методы, при использовании которых имеется возможность приблизить обучающегося к производственной ситуации наиболее реалистично. Всем этим требованиям в наибольшей степени отвечают деловые игры [1]. Отсутствие методических материалов для обучения студентов с использованием деловых игр делает актуальной задачу по разработке как учебных материалов, так и игровых программ [2].

Постановка и решение задачи

В качестве контрольного задания рассматривается задача по изучению и проектированию систем ИБ. Обучающемуся предлагается объект защиты, для которого необходимо спроектировать систему ИБ или, при ее наличии и необходимости, усовершенствовать. Целью проектирования системы ИБ является выработка рекомендаций, организационных и технических решений по обеспечению безопасности информационных ресурсов, хранимых, обрабатываемых и передаваемых по каналам связи в компьютерных сетях и информационных системах (ИС) организации.

Характеристики объекта защиты

Под объектом защиты будем понимать информацию, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации [3].

По результатам анализа требований нормативных документов в области ИБ (Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК) России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и др.) выделим следующие основные характеристики объекта защиты:

- характер информации, подлежащей защите (персональные данные; информация, обрабатываемая в государственных ИС);
- архитектура ИС обработки защищаемой информации (клиент-серверная – «тонкий» клиент, «толстый» клиент; файл-серверная);
- структура ИС обработки защищаемой информации (автономные рабочие места, локальная ИС, распределенная ИС – используемое сетевое оборудование);
- наличие подключений ИС к локальной вычислительной сети (ЛВС) организации или сетям международного информационного обмена;
- наличие системы защиты информации (специализированное программное обеспечение для защиты от несанкционированного доступа (НСД) к информации, средства защиты системы управления базами данных);
- количество технических средств, обрабатывающих защищаемую информацию;
- количество помещений, в которых обрабатывается информация, подлежащая защите;
- наличие физической защиты и ее основные характеристики (наличие жалюзи на окнах, наличие решеток на окнах, опечатывание помещения, охранная сигнализация, пожарная сигнализация);
- наличие сотрудника, занимающегося обеспечением ИБ;
- наличие сотрудников, обеспечивающих предоставление всей необходимой информации.

Представленный перечень характеристик объекта защиты не является полным, указанные характеристики используются в качестве критериев формирования объекта защиты для изучения предметной области.

Преподаватель, выбирая те или иные значения перечисленных выше характеристик объекта защиты, формирует задание на изучение или проектирование системы ИБ.

Предлагаются три типа заданий:

- на проектирование системы ИБ;
- на изучение и дальнейшую модернизацию уже имеющейся системы ИБ;

- только на изучение имеющейся системы ИБ.

Введем три уровня сложности заданий: базовый, повышенный и высокий. Выполнение заданий соответствующего уровня сложности характеризует соответствующий уровень подготовки обучающегося.

Проведение обучающимся обследования объекта защиты

Обследование объекта защиты позволяет получить наиболее полную и объективную оценку защищенности ИС, локализовать имеющиеся проблемы и разработать эффективную программу построения системы обеспечения ИБ организации.

На данном этапе осуществляется сбор необходимой информации и анализ организационных, программных, программно-аппаратных и технических мер обеспечения безопасности информации, предпринятых в организации.

Выявленные характеристики представлены в таблице.

Сведения	Источник получения информации	Раздел в документе		
		Технический паспорт	Разрешительная система доступа	Частная модель угроз
Архитектура и конфигурация ИС обработки защищаемой информации	Персонал организации. Технические средства обработки информации (рабочие места пользователей)	Структура, топология и размещение основных технических средств и систем относительно границ контролируемой зоны объекта	Разрешительная система доступа к информационным (программным) ресурсам	Угрозы НСД в ИС персональных данных. Угрозы НСД по каналам связи

Организационные меры носят административный и процедурный характер и регламентируют процессы функционирования ИС, обработку защищаемой информации и действия персонала.

Таким образом, необходимо проанализировать следующие организационные характеристики:

- наличие, полнота и актуальность организационно-регламентных и нормативно-технических документов;
- разделение зон ответственности ролей персонала по обеспечению ИБ и его корректность;
- наличие документированных списков, описывающих полномочия сотрудников по доступу к защищаемой информации;
- осведомленность пользователей и персонала, поддерживающего функционирование ИС, о требованиях по обеспечению ИБ;
- порядок предоставления доступа к внутренним ресурсам ИС.

В ходе изучения программных, программно-аппаратных и технических мер обеспечения безопасности информации необходимо:

- определить версию и конфигурацию операционной системы;
- определить перечень используемых программных средств;
- выявить наличие программных или программно-аппаратных средств защиты информации (СЗИ);
- выявить наличие сертификатов соответствия используемых СЗИ;
- выявить наличие оперативного анализа журналов аудита и реагирования на события, связанные с попытками НСД;
- выявить наличие процедур по обнаружению и фиксации инцидентов ИБ;
- выявить наличие процедуры документирования любых действий, связанных с модификацией прав доступа, изменениями параметров аудита;
- проверить корректность процедур управления изменениями и установления обновлений;
- выявить наличие механизмов разграничения доступа к документации;
- выявить наличие антивирусной проверки трафика, а также антивирусного контроля на рабочих станциях пользователей;
- выявить наличие резервных копий файлов конфигурации и образов дисков для критичных сетевых устройств и серверов;
- выявить наличие средств для организации контроля доступа и разграничения полномочий пользователей;

- выявить наличие аппаратных ключей доступа и криптографических СЗИ (СКЗИ);
- определить топологию и конфигурацию ИС обработки защищаемой информации;
- изучить условия расположения объекта защиты и определить границы контролируемой зоны;
- определить состав технических средств, используемых для обработки, передачи и хранения защищаемой информации, с указанием категории, заводских номеров, модели, изготовителя, номеров сертификатов соответствия и мест установки;
- выявить наличие пломб (печатей) на технических средствах (системный блок рабочей станции);
- выявить наличие средств физической безопасности помещений, в которых производится обработка защищаемой информации.

Источники получения информации

К источникам получения информации относятся:

- персонал организации;
- технические средства обработки информации (ТСОИ);
- помещение, в котором производится обработка защищаемой информации.

Персонал организации представлен:

1. Пользователями. К ним относятся сотрудники структурного подразделения, обрабатывающего защищаемую информацию. Сотрудники структурных подразделений в рамках своих компетенций предоставляют данные по текущему состоянию объекта защиты. Зачастую пользователи хорошо осведомлены только в вопросах своей специальности.

2. Системным администратором. Это сотрудник, должностные обязанности которого подразумевают обеспечение штатной работы парка компьютерной техники, сети и программного обеспечения.

3. Пользователями СКЗИ. К ним относятся сотрудники, назначенные ответственными за использование СКЗИ, в должностные обязанности которых входит обеспечение функционирования и безопасности криптосредств и ключевых документов к ним.

4. Администратором безопасности информации (или специалистом по защите информации). Это сотрудник, в должностные обязанности которого входит обеспечение ИБ. Однако данный специалист также должен быть хорошо осведомлен в вопросах работы сети и программного обеспечения.

С помощью опроса персонала организации можно получить некоторые сведения об объекте защиты информации. Каждая группа пользователей имеет определенный уровень знаний о данном объекте.

Пример составленного дерева вопросов и ответов представлен на рис. 1.

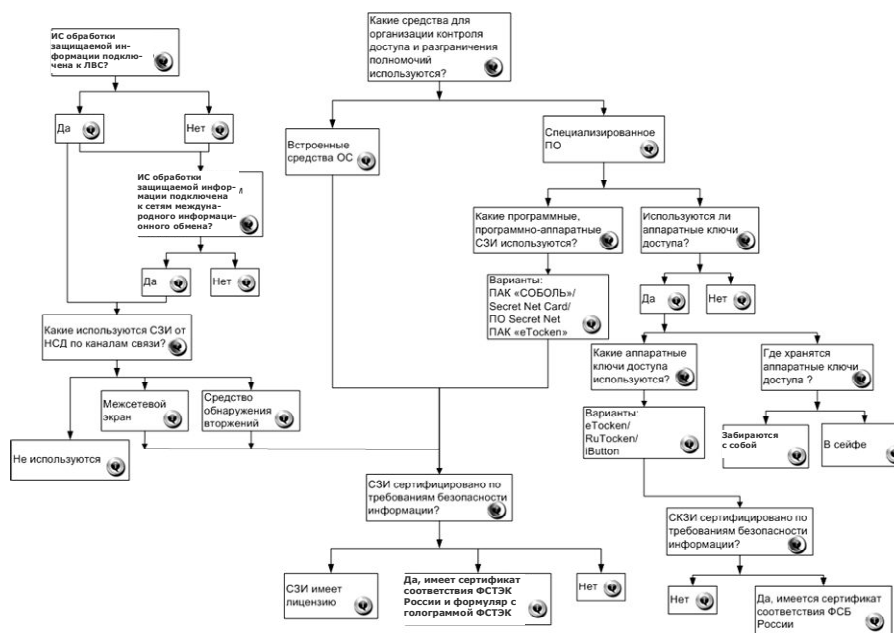


Рис. 1. Дерево вопросов и ответов «Используемые средства защиты информации»

Технические средства обработки информации имеют реальные характеристики и конфигурации, которые можно просмотреть, используя стандартные решения операционной системы.

Формирование объекта защиты

Формирование объекта защиты проводится на основе заданных преподавателем характеристик. Функциональная диаграмма на рис. 2 отражает последовательность выполнения функций для рассматриваемой задачи построения объекта защиты. Очередность выполнения этих функций следующая:

- формирование помещения;
- формирование ИС обработки защищаемой информации;
- генерация технических средств;
- генерация программного обеспечения;
- формирование системы защиты информации;
- комплектация автоматизированного рабочего места (АРМ).

В качестве исходной информации, на основе которой выполняется формирование объекта, используются его характеристики (их значения устанавливаются преподавателем). Результатом является сформированный программой объект защиты.

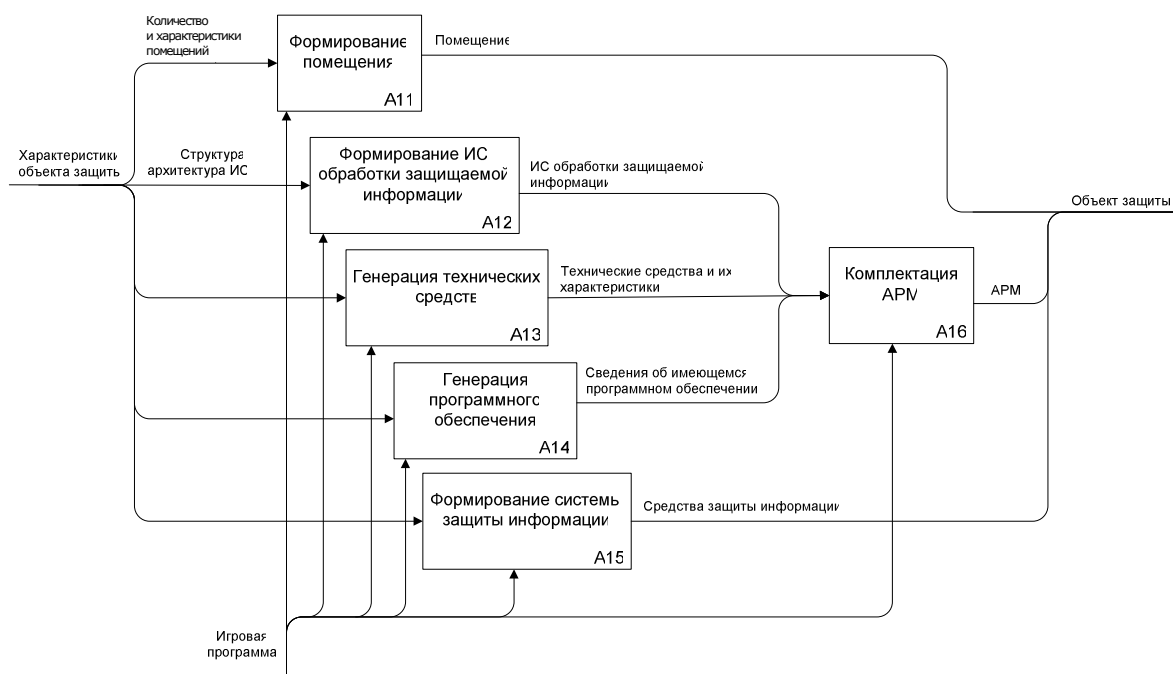


Рис. 2. Функциональная диаграмма «Формирование объекта защиты информации»

Приведенная модель была положена в основу разработанной в среде Visual Studio 2008 и XNA Game Studio 3.1 на языке C# программы, позволяющей генерировать объект защиты информации, представленный в трехмерном режиме [4].

Методика оценки знаний и навыков обучающихся

Результатом обследования объекта защиты информации является формирование следующих документов:

- технический паспорт;
- разрешительная система доступа;
- частная модель угроз безопасности информации.

Соответственно, оценка знаний и навыков обучающихся будет производиться по разработанным обучающимся документам.

Каждый документ состоит из тематических разделов, при формировании которых обучающийся использует информацию, полученную в ходе обследования объекта защиты. Каждому разделу ставится в соответствие вес, или важность в общем документе. Информация, представленная в каждом разделе, оценивается по двум критериям.

В качестве критериев оценки выбраны следующие:

- правильность обследования предметной области – P_0 ;
- правильность заполнения соответствующего раздела документа – P_3 .

Каждый критерий представлен числом от 0 до 1.

Предложенную схему оценки можно представить в виде ориентированного графа (рис. 3).

Оценку раздела документа производим по следующей формуле:

$$K_i = \sum_{j=1}^{m_i} (P_0^{\alpha_{0j}} \cdot P_3^{\alpha_{3j}}) \cdot \beta_{ij},$$

где β_{ij} – важность j -й информации в i -м разделе документа; α_{0j} , α_{3j} – важность критериев P_0 и P_3 соответственно для j -й информации.

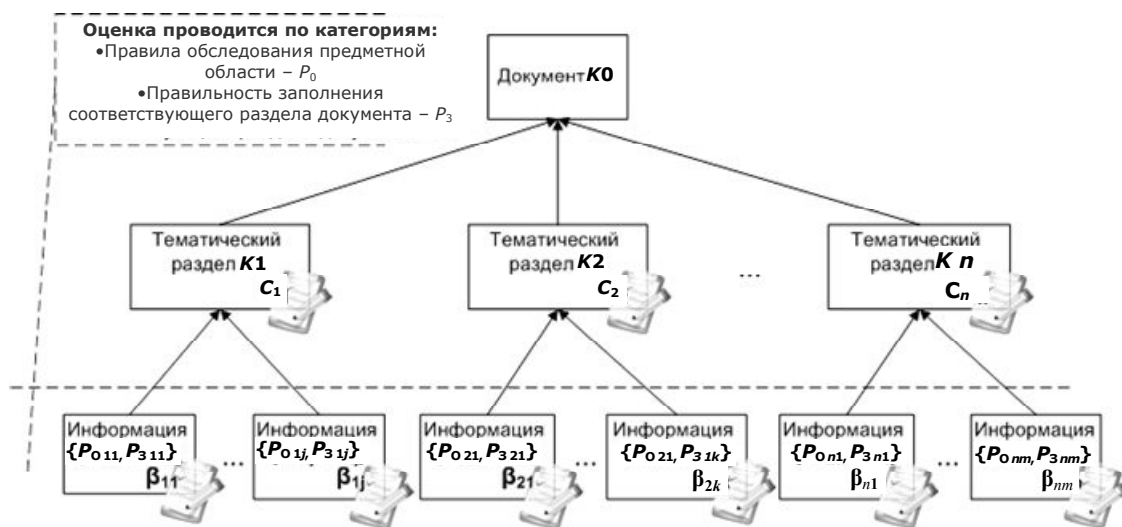


Рис. 3. Схема оценки документа

Для оценки всего документа также применяем аддитивную свертку, и в итоге получаем числовую характеристику уровня подготовки обучающегося:

$$K_{\text{док}} = \sum_j C_j K_{\text{гл}j}.$$

Применение аддитивной свертки в этом случае обусловлено тем, что невысокая оценка одного критерия (например, оценка по одному разделу документа) может быть скомпенсирована высокой оценкой по другому критерию.

Заключение

Таким образом, в ходе исследований был проведен системный анализ объекта защиты информации в соответствии с требованиями нормативных документов в области ИБ, выявлены основные характеристики объекта защиты, необходимые для проведения его предварительного обследования с использованием методов опроса, просмотра его информационных и физических параметров. Предложена методика обучения навыкам проведения обследования объекта защиты, которая позволит сформировать умения и навыки, необходимые в профессиональной деятельности специалиста по защите информации.

Статья поступила в редакцию 31.05.2013

СПИСОК ЛИТЕРАТУРЫ

1. Суворова Н. Интерактивное обучение: Новые подходы / Н. Суворова. – М.: Прогресс, 2005. – 214 с.
2. Наурзбаева А. Х. Игровая программа для изучения и проектирования систем информационной безопасности / А. Х. Наурзбаева А. Х. // Междунар. науч. конф. «Инновационные технологии в управлении, образовании, промышленности» АСТИНТЕХ-2013: докл. молодых ученых в рамках программы «Участник молодежного научно-инновационного конкурса» («У.М.Н.И.К.»), г. Астрахань, 22–24 мая 2013 г. – Астрахань: Изд. дом «Астраханский университет», 2013. – С. 36–37.
3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Взамен ГОСТ Р 50922-96; введ. 2008-02-01. – М.: Стандартинформ, 2008. – 12 с.
4. Свидетельство о государственной регистрации программы для ЭВМ «Подсистема генерации игровой модели объекта защиты» № 2013613713 от 15 апреля 2013 года.

REFERENCES

1. Suvorova N. *Interaktivnoe obuchenie: Novye podkhody* [On-line training. New approaches]. Moscow, Progress Publ., 2005. 214 p.
2. Naurzbaeva A. Kh. *Igrovaia programma dlia izuchenii i proektirovaniia sistem informatsionnoi bezopasnosti* [Game program for studying and designing systems of information security]. *Mezhdunarodnaia nauchnaia konferentsiia «Innovatsionnye tekhnologii v upravlenii, obrazovanii, promyshlennosti» ASTINTEKh-2013. Doklady molodykh uchenykh v ramkakh programmy «Uchastnik molodezhnogo nauchno-innovatsionnogo konkursa» («U.M.N.I.K.»)*, g. Astrakhan', 22–24 maia 2013 g. Astrakhan, Izdatel'skii dom «Astrakhanskii universitet», 2013, pp. 36–37.
3. *GOST R 50922-2006. Zashchita informatsii. Osnovnye terminy i opredeleniia* [Information protection. The main terms and definitions]. *Vzamen GOST R 50922-96; vved. 2008-02-01*. Moscow, Standartinform, 2008. 12 p.
4. *Svidetel'stvo o gosudarstvennoi registratsii programmy dlia EVM «Podsistema generatsii igrovoi modeli ob"ekta zashchity»* № 2013613713 ot 15 apreliia 2013 goda [License on state registration of the program for IBM "Subsystem of generation of playing model of an object of protection"].

ИНФОРМАЦИЯ ОБ АВТОРАХ

Белов Сергей Валерьевич – Астраханский государственный технический университет; канд. техн. наук, доцент; доцент кафедры «Информационная безопасность»; ssbelov@yandex.ru.

Belov Sergey Valerievich – Astrakhan State Technical University, Candidate of Technical Sciences, Assistant Professor; Assistant Professor of the Department "Information Security"; ssbelov@yandex.ru.

Наурзбаева Алия Хаиржановна – Астраханский государственный технический университет; студентка, специальность «Комплексное обеспечение информационной безопасности автоматизированных систем»; naurzbaeva_aliya@mail.ru.

Naurzbaeva Aliya Khairzhanovna – Astrakhan State Technical University; Student, Specialty "Complex Support of Information Security of Automated Systems"; naurzbaeva_aliya@mail.ru.