7. Shkurina G. L. Ispolzovanie protsedur vybora dlya postroeniya ocheredey remonta oborudovaniya [Use of choice procedure for creation turns of equipment repair]. Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki [Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics], 2011, no. 3 (73), pp. 74–78.

8. Kandyrin Y. W., Rörs G. Interaktive und automatische Recherche von Invormationen für den Konstrukteur. Wissenschaftliche Zeitschrift der Technische Universität Dresden, 1984, h. 2, no. 33, s. 147–151.

9. Levitin A., Anany V. Introduction to the Design & Analysis of Algorithms. M., Vilyams, 2006, p. 1296. ISBN 0-07-013151-1.

10. Tanino N., Sawaragi Y. Stability of nondominated solutions in multicriteria decision-making. *J. Opt. Theory and Appl.*, 1980, vol. 30, no. 2, pp. 229–253.

УДК 004.056

МЕТОДИКА ОЦЕНКИ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВУЗА И ЕЕ АПРОБАЦИЯ НА ПРИМЕРЕ АСТРАХАНСКОГО ГОСУДАРСТВЕННОГО ТЕХНИЧЕСКОГО УНИВЕРСИТЕТА

Статья поступила в редакцию 27.12.2013, в окончательном варианте 14.01.2014.

Ажмухамедов Искандар Маратович, кандидат технических наук, доцент, Астраханский государственный технический университет, 414025, Российская Федерация, г. Астрахань, ул. Татищева, 16, e-mail: aim_agtu@mail.ru

Учаев Дмитрий Юрьевич, ведущий программист, Астраханский государственный технический университет, 414025, Российская Федерация, г. Астрахань, ул. Татищева, 16, e-mail: uchaevdyu@icloud.com

Ажмухамедов Альберт Искандарович, аспирант, Астраханский государственный технический университет, 414025, Российская Федерация, г. Астрахань, ул. Татищева, 16, e-mail: bert91@mail.ru

Авторами построена нечеткая когнитивная модель оценки уровня информационной безопасности (ИБ) вуза, которая позволяет связать данные по составу угроз, уязвимостей, средств защиты между собой и рассмотреть влияние потенциально возможных атак на основные сервисы безопасности информационных активов учебного заведения. Нечеткая когнитивная модель не только обеспечивает оценку уровня информационной безопасности, но и дает возможность выработать рекомендации по его повышению, более целенаправленно проводить поиск уязвимостей системы защиты информации, а также аккумулировать полученные при этом знания. Проверка адекватности разработанной модели была осуществлена на примере Астраханского государственного технического университета. Проверка показала достаточно хорошее соответствие между теоретическими результатами и данными реального тестирования системы обеспечения информационной безопасности, проведенного специально подобранной командой. Разработанная авторами методика может быть применена для оценки уровня ИБ высших учебных заведений.

Ключевые слова: информационная безопасность, нечеткая когнитивная модель, атака на информационные ресурсы, защита информации, информационный актив, безопасность вуза, свертка векторного критерия, нечеткий классификатор

PRIKASPIYSKIY ZHURNAL: Upravlenie i Vysokie Tekhnologii
(CASPIAN JOURNAL: Management and High Technologies), 2014, 1 (25)
SYSTEM ANALYSIS, MODELS AND METHODS OF DECISION-MAKING,
MANAGEMENT IN CLEAR AND FUZZY TERMS

EVALUATION OF THE LEVEL OF UNIVERSITY INFORMATION SECURITY AND ITS APPROBATION BY THE EXAMPLE OF ASTRAKHAN STATE TECHNICAL UNIVERSITY

Azhmukhamedov Iskandar M., Ph.D. (Engineering), Associate Professor, Astrakhan State Technical University, 16 Tatishchev St., Astrakhan, 414025, Russian Federation, e-mail: aim_agtu@mail.ru

Uchaev Dmitriy Yu., Leading Programmer, Astrakhan State Technical University, 16 Tatishchev St., Astrakhan, 414025, Russian Federation, e-mail: uchaevdyu@icloud.com

Azhmukhamedov Albert I., post-graduate student, Astrakhan State Technical University, 16 Tatishchev St., Astrakhan, 414025, Russian Federation, e-mail: bert91@mail.ru

The authors constructed a fuzzy cognitive model (FCM) assess the information security level (IS), which allows you to link data on the composition of threats, vulnerabilities, means of protection between themselves and consider the impact of potential attacks on basic security services institution's information assets. FCM not only provides an assessment of the level of information security, but also gives the opportunity to develop recommendations for improved, more targeted search for information security vulnerabilities, as well as accumulate this knowledge. Assesses the adequacy of the developed model was implemented on the example of the Astrakhan State Technical University and showed good correspondence between the theoretical results and data of real test information security University, conducted by a specially selected team.

Keywords: information security, fuzzy cognitive model, attack on information resources, information protection, information asse, university security, folding vector criterion, fuzzy classifier

Введение. Российская высшая школа в настоящее время переживает период адаптации к новым социально-экономическим условиям с разноплановыми проявлениями конкурентной борьбы. Такая адаптация требует создания эффективных механизмов управления информационными ресурсами системы высшего образования, научного обоснования и практической реализации сбалансированной политики информационной безопасности (ИБ) [5].

Специфика защиты информации (ЗИ) в вузе связана с многопрофильным характером его деятельности, обилием форм и методов учебной и научной работы, пространственной распределенностью инфраструктуры (корпуса, филиалы, представительства). Сюда же можно отнести и многообразие источников финансирования, наличие большого количества вспомогательных подразделений и служб, необходимость адаптации к меняющемуся рынку образовательных услуг, отсутствие общепринятой формализации деловых процессов, необходимость электронного взаимодействия с вышестоящими организациями, частое изменение статуса сотрудников и обучаемых. Кроме того, вуз – это публичное заведение с непостоянной аудиторией, а также место повышенной активности «начинающих киберпреступников» [10].

Таким образом, высшие учебные заведения обладают рядом особенностей, которые необходимо учесть при построении комплексной системы обеспечения информационной безопасности (КОИБ).

Под термином «информационная безопасность» вуза в соответствии с [7] мы будем понимать состояние защищенности интересов организации в условиях угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств (сервисов) ИБ – конфиденциальностью, целостностью, доступностью информационных активов организации.

Информационные активы – это «информационные ресурсы, в том числе различные виды информации, циркулирующие в информационной системе (служебная, управляющая, аналитическая, деловая и т.д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение) или средства обработки информации» [7, 13].

Постановка задачи. Исходя из вышеизложенного, для оценки уровня ИБ вуза необходимо связать данные по составу угроз, уязвимостей, средств защиты друг с другом и рассмотреть влияние потенциально возможных атак на основные сервисы безопасности информационных активов.

Анализ состава угроз, уязвимостей и средств защиты. Информационные активы учебного заведения подвержены следующим типам угроз:

- *непреднамеренные субъективные угрозы* (неумышленное повреждение или отключение оборудования; неумышленное удаление или искажение файлов с важной информацией; неумышленное удаление программ; порча носителей информации, ввод ошибочных данных и т.п.);
- *преднамеренные субъективные угрозы* (преднамеренное физическое разрушение системы; вывод из строя наиболее важных компонентов информационной системы (ИС), отключение подсистем инженерного обеспечения, преднамеренное нарушение режимов эксплуатации устройств или режимов использования программного обеспечения (ПО), хищение носителей информации и т.п.);
- *техногенные угрозы* (сбой или отказ технических средств обработки информации, вспомогательных технических средств, систем электроснабжения, климат-контроля и т.п.);
- *стихийные угрозы* (пожар, наводнение, землетрясение, пыльные бури, экстремально высокая/низкая температура и т.п.).

Перечисленные угрозы (обозначим их совокупность как $\{UG_j\}_{j=1...J}$, где J – общее количество видов угроз) имеют априорные вероятности возникновения, зависящие от различных параметров: привлекательности информационного актива для злоумышленника, уровня его квалификации (для субъективных угроз); состояния внешней инфраструктуры, окружающей объект информатизации, его расположения, климатических условий и т.д. Любая из угроз множества $\{UG_j\}_{j=1...J}$ может реализоваться в виде атаки на информационные активы при наличии соответствующей уязвимости [8].

К основным уязвимостям $\{UZ_k\}_{k=1...K}$ систем обеспечения ИБ образовательных учреждений можно отнести: отсутствие утверждённой концепции ИБ; низкую надежность основных и вспомогательных технических средств (ТС); наличие ошибок в программном обеспечении; несоблюдение режима охраны; нештатные режимы использования ПО и эксплуатации ТС и т.д.

В качестве средств защиты информации, образующих множество мер противодействия $\{Z_i\}_{i=1...I}$, обычно используют: эффективную организацию процедуры хранения документов; разработку мер оперативного реагирования на инциденты; административные и технические средства контроля за работой пользователей; использование только сертифицированного лицензионного ПО; разграничение прав доступа к ПО; периодическое резервное копирование информации; обучение сотрудников основам ИБ; формирование культуры безопасного поведения в информационном пространстве и т.д.

Структура нечеткой когнитивной модели оценки уровня информационной безопасности вуза. Поскольку большинство задач, возникающих в процессе обеспечения ИБ, представляют собой ярко выраженные плохо формализуемые проблемы, то для их описания и анализа целесообразно применение аппарата нечеткого когнитивного моделирования, который по сравнению с другими методами дает возможность формализации численно неизмеримых факторов, позволяет использовать неполную, нечеткую и даже противоречивую информацию [9, 16].

При построении нечеткой когнитивной модели (НКМ) оценки уровня информационной безопасности необходимо связать основные концепты рассматриваемой проблемы в рамках нечеткого графа G [1].

При этом на нижнем уровне иерархии располагаются средства и механизмы защиты ***Z***, действия которых уменьшают вероятности возникновения угроз ***UG*** и ослабляют степени уязвимостей ***UZ***, расположенных на уровень выше. Угрозы и уязвимости, в свою очередь, определяют вероятность возникновения атак A, которые негативно влияют на сервисы безопасности ***SRV*** (конфиденциальность, целостность, доступность).

Эти сервисы в совокупности определяют интегральный показатель комплексной ИБ учебного заведения ***K*** и влияют на репутацию вуза, его материально-техническое состояние, финансовую устойчивость, качество образовательного процесса, эффективность научных исследований и т.п.

В построенной таким образом НКМ все значения концептов, входящих в нечеткий граф ***G***, задаются с помощью лингвистической переменной «Уровень фактора» с термножеством:

$$QL = \{\text{Низкий (}\mathbf{H}\text{), Ниже среднего (}\mathbf{HC}\text{), Средний (}\mathbf{C}\text{),}$$
$$\text{Выше среднего (}\mathbf{BC}\text{), Высокий (}\mathbf{B}\text{)}\} \quad (1)$$

В качестве семейства функций принадлежности выступает стандартный пятиуровневый 01-классификатор, где функции принадлежности μ_F – трапецеидальные нечеткие числа (НЧ) [11, 12, 15]:

$$\mathbf{H}\ (0;\ 0;\ 0{,}15;\ 0{,}25);\ \mathbf{HC}\ (0{,}15;\ 0{,}25;\ 0{,}35;\ 0{,}45);\ \mathbf{C}\ (0{,}35;\ 0{,}45;\ 0{,}55;\ 0{,}65);$$
$$\mathbf{BC}\ (0{,}55;\ 0{,}65;\ 0{,}75;\ 0{,}85);\ \mathbf{B}\ (0{,}75;\ 0{,}85;\ 1;\ 1), \quad (2)$$

где в нечетком числе $\mathbf{X}(a_1, a_2, a_3, a_4)$: a_1 и a_4 – абсциссы нижнего основания; a_2 и a_3 – абсциссы верхнего основания трапеции (рис. 1).

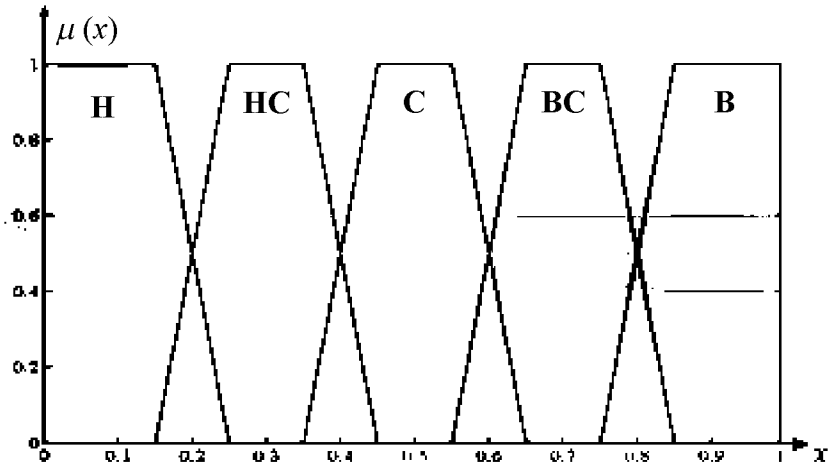

Рис. 1. Система трапецеидальных функций принадлежности
на 01-носителе (пятиуровневый 01-классификатор)

Для осуществления вычислений с нечеткими числами используется принцип расширения арифметических операций, предложенный Л. Заде [6].

Значения концептов НКМ находятся по следующим формулам:

$$\overline{UZ}_j^{mn} = UZ_j^{mn} \cdot \prod_i Inv(Z_i^{mn})^{r_i^{mn}}, \quad (3)$$

$$\overline{UZ}^{mn} = Inv\left[\prod_j Inv\left(\overline{UZ}_j^{mn}\right)^{s_j^{mn}}\right], \quad (4)$$

$$\overline{UG}_n^m = UG_n^m \cdot \prod_i Inv(Z_i^{mn})^{v_i^{mn}}, \quad (5)$$

где $Inv(F) = 1 - \mu_F$ – инверсия фактора F (μ_F – функция принадлежности для фактора F); $\overline{UZ}_j^{mn}$ – остаточный (после применения средств защиты) уровень j-й уязвимости m-го актива относительно n-ой угрозы; UZ_j^{mn} – исходный (до применения средств защиты) уровень j-й уязвимости m-го актива относительно n-й угрозы; Z_i^{mn} – уровень i-ой защитной меры по отношению к n-й угрозе m-му активу; r_i^{mn} – весовой коэффициент, отражающий «вклад» i-й защитной меры в снижение уровня n-ой угрозы m-у активу; $\overline{UZ}_j^{mn}$ – интегральный уровень уязвимости m-го актива по отношению к n-й угрозе; s_j^{mn} – весовой коэффициент, отражающий «вклад» $\overline{UZ}_j^{mn}$ в $\overline{UZ}^{mn}$; $\overline{UG}_n^m$ – остаточная вероятность существования угрозы UG_n для m-го актива после применения совокупности средств защиты Z_i^{mn}; UG_n^m – исходная вероятность существования угрозы UG_n для m-го актива; v_i^{mn} – весовой коэффициент, отражающий «вклад» элемента защиты Z_i^{mn} в уменьшение угрозы UG_n^m.

Результат нахождения сверток векторного критерия в иерархии $\boldsymbol{G}$ является нечетким числом, которое необходимо лингвистически распознать, чтобы выработать суждение о качественном уровне показателей. Для этого вычисляется индекс схожести Ω, характеризующий степень соответствия значения фактора той или иной качественной оценке из терм-множества лингвистической переменной QL (1):

$$\Omega = (1 + \tilde{\rho})/2 \tag{6}$$

$$\tilde{\rho} = (\rho_{in} - \rho_{out})/(\rho_{in} + \rho_{out}), \tag{7}$$

где

$$\rho_{in} = \int_{c_1}^{c_4} (\min[\mu_B(x); \mu_C(x)])dx; \qquad \rho_{out} = \left| \int_{b_1}^{b_4} [\mu_B(x)]dx - \rho_{in} \right|; \tag{8}$$

(ρ_{out} представляет собой площадь НЧ $B(b_1, b_2, b_3, b_4)$, характеризующего результат, лежащую вне эталонного нечеткого числа $C(c_1, c_2, c_3, c_4)$, а ρ_{in} – площадь, лежащую внутри этого же НЧ; $\mu_B(x)$ и $\mu_C(x)$ – функции принадлежности соответствующих нечетких чисел).

Определенный таким образом индекс схожести, изменяясь в диапазоне от 0 до 1, характеризует близость найденной свертки к тому или иному нечеткому числу, которое, в свою очередь, соответствует элементу эталонного терм-множества.

При этом обеспечивается семантическое соответствие: чем больше индекс схожести, тем выше степень соответствия вычисленного значения одному из элементов терм-множества $\boldsymbol{QL}$.

Разница индексов схожести качественных оценок, полученных экспериментальным и теоретическим путем, может быть использована в качестве метрической характеристики степени адекватности нечеткой когнитивной модели.

Реализация n-ой угрозы m-му активу $\overline{UG}_n^m$ через имеющиеся уязвимости $\overline{UZ}^{mn}$ соответствует атаке A_n^m, вероятная результативность которой может быть оценена по формуле:

$$A_n^m = \overline{UG}_n^m \cdot \overline{UZ}^{mn}. \tag{9}$$

Если данная величина отлична от нуля, т.е. несмотря на предпринятые защитные мероприятия, в некоторый момент времени t^{mn} атака A_n^m все же возникла, то задействуются меры $\{Z_i^{mn}\}$ по снижению уровня нарушений безопасности (инцидентов).

Данные меры могут быть активизированы не сразу, а спустя некоторое время $(t_j^{mn})_{\text{нач}}$, необходимое для идентификации атаки и принятия решения о реагировании на нее. При достижении времени $(t_j^{mn})_{\text{кон}}$ действие этих мер прекращается – либо в связи с окончанием инцидента, либо в связи с исчерпанием ресурсов, обеспечивающих сдерживание атаки.

Во время действия данных мер результативность *n*-ой атаки на *m*-ый ресурс $\overline{A}_n^m$ может быть найдена по формуле:

$$\overline{A}_n^m = A_n^m \cdot \prod_j Inv\left(Z_j^{mn}\right)^{\gamma_j^{mn}}, \tag{10}$$

где γ_j^{mn} – весовой коэффициент, отражающий вклад меры Z_j^{mn} в снижение уровня *n*-го инцидента (атаки) по отношению к *m*-му активу.

Инциденты ИБ при условии, что их уровень выше некоторого критического порога $(\overline{A}_n^m)_{\text{крит}}$ и продолжительность больше некоторого критического интервала времени $(t_j^{mn})_{\text{крит}}$, могут порождать новые или усиливать уже имеющиеся уязвимости системы, что должно найти отражение при оценке их уровня на следующем шаге по времени:

$$UZ_j^{mn}(t+\Delta t) = UZ_j^{mn}(t) \cdot Inv\left[\prod_n Inv(\overline{A}_n^m)^{\delta_j^{mn}}\right]. \tag{11}$$

Совокупность атак на *m*-ый информационный актив, в свою очередь, определяет уровень обеспеченности сервисов безопасности данного актива SRV_k^m:

$$SRV_k^m = \prod_n Inv(\overline{A}_n^m)^{w_n^{mk}}. \tag{12}$$

Если уровень какого-либо сервиса падает ниже критического значения, то необходимо предпринять меры по его восстановлению, т.е. реализовать мероприятия блока ликвидации последствий [2]. Результат действий на этом шаге формализуется с помощью следующей формулы:

$$\overline{SRV}_k^m = SRV_k^m \cdot Inv\left[\prod_j Inv(Z_j^{mk})^{\theta_j^{mk}}\right], \tag{13}$$

где $\overline{SRV}_k^m$ – уровень *k*-го сервиса *m*-го актива после реализации мер ликвидации последствий Z_j^{mk}; θ_j^{mk} – весовой коэффициент, отражающий вклад меры Z_j^{mk} в повышение уровня *k*-го сервиса безопасности *m*-го актива.

Так же как и в случае с мерами по снижению уровня инцидентов, до активизации данных мер проходит некоторое время $(t_j^{mk})_{\text{нач}}$, необходимое для идентификации уровня сервисов безопасности и принятия решения о необходимости их повышения. Действие этих мер прекращается в некоторый момент времени $(t_j^{mk})_{\text{кон}}$ либо в связи с достижением нужного уровня сервиса безопасности, либо в связи с исчерпанием ресурсов для его повышения.

Основываясь на значениях сервисов безопасности $\overline{SRV}_k^m$ для m-го актива, определяется интегральный уровень его безопасности K^m:

$$K^m = \prod_k (\overline{SRV}_k^m)^{a_k^m}, \quad (14)$$

где a_k^m – весовой коэффициент, отражающий «вклад» k-го сервиса в интегральную оценку уровня безопасности m-го актива.

Обобщенный показатель K комплексной безопасности всего учебного заведения находится по формуле:

$$K = \prod_m (K^m)^{\beta_m}, \quad (15)$$

где β_m – весовой коэффициент, отражающий значимость m-го информационного актива в обобщенной оценке комплексного уровня безопасности образовательного учреждения.

Применение мультипликативной свертки в формуле (15) обусловлено тем, что каждый из частных критериев K^m критично значим при определении обобщенного показателя K и взаимная компенсация низких значений одних критериев за счет высоких значений других (как это имеет место, например, при аддитивной свертке) не допускается. Значение мультипликативного критерия, в отличие от аддитивного, резко уменьшается при малых значениях отдельных критериев, что позволяет лучше учесть их влияние.

Тестирование уровня информационной безопасности АГТУ. Проверка адекватности предложенной модели была осуществлена в рамках решения задачи комплексной оценки уровня информационной безопасности ФГБОУ ВПО «Астраханский государственный технический университет (АГТУ)».

Для этого были выделены и проранжированы по степени значимости информационные активы, которые могут быть подвержены атакам.

Из множеств ***UG*** и ***UZ*** были отобраны угрозы и уязвимости, характерные для каждого из видов активов. Затем был составлен перечень имеющихся в вузе средств обеспечения ИБ и проанализировано влияние использования этих средств на угрозы и уязвимости, выявленные на предыдущем этапе.

При имеющихся в АГТУ средствах ЗИ интегральный уровень ИБ K_0 при помощи приведенной выше нечеткой когнитивной модели был оценен как «средний» с индексом схожести $\Omega = 0{,}78$.

С целью проверки адекватности полученной оценки из общего перечня субъективных угроз, содержащего 45 пунктов [14], были выбраны 13 угроз, направленных на основные сервисы безопасности (конфиденциальность, целостность, доступность) наиболее значимых информационных активов АГТУ:

- UG_{23} – вывод из строя наиболее важных компонентов ИС;
- UG_{24} – отключение подсистем обеспечения ИС;
- UG_{26} – преднамеренное нарушение режимов эксплуатации устройств или режимов использования ПО;
- UG_{32} – перехват информации в каналах связи и их анализ;
- $UG33$ – осуществление «маскарада» (выполнения действий под видом другого пользователя или другой системы);
- UG_{34} – хищение носителей информации;
- UG_{35} – несанкционированное копирование информации;
- UG_{38} – чтение остаточной информации с внешних ЗУ;
- UG_{39} – незаконное получение реквизитов разграничения доступа;

- UG_{40} – вскрытие шифров криптозащиты информации;
- UG_{42} – внедрение программных «закладок» и «вирусов»;
- UG_{44} – навязывание ложных сообщений (фальсификация);
- UG_{45} – модификация потока данных.

Для каждой из отобранных угроз экспертной группой, в состав которой вошли преподаватели кафедры ИБ АГТУ, представители ФСТЭК по Астраханской области и представитель ФГУП «ЦентрИнформ», были выявлены необходимые для их реализации компетенции «злоумышленника»:

- $К_1$ – навыки использования специального ПО для перехвата и модификации потока данных;
- $К_2$ – знание протоколов обмена данными МЕЖДУ ЧЕМ И ЧЕМ;
- $К_3$ – знание теории кодирования;
- $К_4$ – знание топологии сетей передачи данных;
- $К_5$ – навыки программирования;
- $К_6$ – навыки социальной инженерии;
- $К_7$ – знание криптографических методов защиты информации;
- $К_8$ – знание систем управления базами данных;
- $К_9$ – навыки использования специального ПО для маскировки;
- $К_{10}$ – знание особенности функционирования различных сетей;
- $К_{11}$ – знание механизмов взаимной аутентификации в сети;
- $К_{12}$ – навыки в написании и отладке «вирусов» и «закладок»;
- $К_{13}$ – знание особенностей функционирования операционных систем;
- $К_{14}$ – навыки использования специального ПО по внедрению «вирусов» и «закладок»;
- $К_{15}$ – знание основ криптоанализа;
- $К_{16}$ – умение работать со специальным ПО для криптоанализа;
- $К_{17}$ – знание основ электротехники и навыки работы с электрооборудованием и электрическими сетями;
- $К_{18}$ – знание основ схемотехники, умение «читать» схемы;
- $К_{19}$ – навыки конфигурирования устройств КАКИХ;
- $К_{20}$ – навыки конфигурирования ПО;
- $К_{21}$ – навыки работы со штатными утилитами для копирования информации;
- $К_{22}$ – умение работать со специальным ПО для несанкционированного копирования информации;
- $К_{23}$ – навыки работы со штатными утилитами восстановления информации;
- $К_{24}$ – умение работать со специальным ПО для восстановления информации;
- $К_{25}$ – навыки работы со специальным ПО для «взлома» паролей;
- $К_{26}$ – знание технологий формирования ключевой информации;
- $К_{27}$ – умение применять приемы социальной инженерии для доступа к конфиденциальной информации;
- $К_{28}$ – умение преодолевать механизмы инженерно-технической защиты.

Далее экспертами были определены необходимые пороговые (минимальные) уровни этих компетенций (табл. 1).

Таблица 1

Минимальные уровни компетенций, необходимые для реализации угроз

	UG_{23}	UG_{24}	UG_{26}	UG_{32}	UG_{33}	UG_{34}	UG_{35}	UG_{38}	UG_{39}	UG_{40}	UG_{42}	UG_{44}	UG_{45}	K_i*
K_1				ВС									В	В
K_2				ВС	С							ВС	ВС	ВС
K_3				НС									С	С
K_4				НС									С	С
K_5											В		ВС	В
K_6	С				В	С	С		В			ВС		В
K_7				С						В		ВС		В
K_8												С		С
K_9				ВС								ВС		ВС
K_{10}												ВС		ВС
K_{11}					В							В		В
K_{12}											В			В
K_{13}							В				В			В
K_{14}											ВС			ВС
K_{15}										В				В
K_{16}										ВС				ВС
K_{17}		С												С
K_{18}			ВС											ВС
K_{19}			ВС											ВС
K_{20}			ВС											ВС
K_{21}							С							С
K_{22}							ВС							ВС
K_{23}								ВС						ВС
K_{24}								ВС						ВС
K_{25}									ВС					ВС
K_{26}									В					В
K_{27}		С				ВС	ВС		ВС			ВС		ВС
K_{28}	ВС	С		С		С	С		ВС					ВС

В табл. 1 через K_i* обозначен пороговый уровень i-ой компетенции, необходимой для выполнения общей задачи (реализация антропогенных угроз по отношению к информационным активам АГТУ).

Для имитации антропогенных (субъективных) угроз была подобрана команда, состоящая из студентов старших курсов специальности «Комплексное обеспечение информационной безопасности автоматизированных систем», преподавателей кафедры «Информационная безопасность» и специалистов отдела «Информационная безопасность» АГТУ.

Формирование команды было осуществлено с помощью процедуры, предусматривающей два этапа [3]. На первом – оценивался уровень компетенций каждого из претендентов. На втором – на основе полученных данных отбирался наиболее подходящий состав исполнителей. ЧТО БЫЛО КРИТЕРИЕМ ОПТИМАЛЬНОСТИ И ОГРАНИЧЕНИЯМИ. В ЧАСТНОСТИ, СТАВИЛАСЬ ЛИ ЦЕЛЬ, ЧТОБЫ ЛЮДИ БЫЛИ ИЗ ВСЕХ ТРЕХ ГРУПП.

С использованием описанной методики путем тестирования и анализа достижений 22 претендентов в различных областях были определены уровни их компетенций и сформирована команда из 8-ми участников (двое преподавателей кафедры, представитель отдела ИБ, пятеро студентов), которая всесторонне протестировала систему комплексного обеспечения ИБ АГТУ.

В силу ограниченных размеров статьи ниже в качестве примера приведено краткое описание только одной из успешных атак на электронные информационные активы университета.

Атака была основана на получении доступа к информационным ресурсам вуза с компьютера, находящегося в локальной сети учебного заведения.

С этой целью в одной из компьютерных аудиторий АГТУ было установлено необходимое программное обеспечение для осуществления атаки и произведено сканирование хостов локальной сети для выявления перспективных для дальнейшей «разработки» IP адресов.

Взлом отобранных на первом этапе информационных активов, размещенных по этим адресам, осуществлялся путем реализации атаки «ARP Poison Routing» («отравление ARP»). Это одна из разновидностей атаки типа «man-in-the-middle» («человек посередине»). Ее реализация позволяет «прослушивать коммутируемые сети и перехватывать IP-трафик между хостами». Описание подобного рода атак (а часто и готовые программные продукты для их реализации) можно достаточно легко найти в сети Интернет.

Атаки такого рода основаны на манипуляции с кэшем ARP хостов. В IP сетях, когда два хоста хотят обменяться информацией, они должны знать MAC-адреса друг друга. Хост источник проверяет свою таблицу ARP, чтобы узнать, есть ли MAC-адрес, соответствующий IP-адресу хоста назначения. Если нет, то он транслирует ARP запрос ко всей сети, запрашивая MAC-адрес хоста адресата. Поэтому пакет, отправленный в сеть, достигнет каждого хоста в подсети. Однако только хост с IP-адресом, указанным в запросе, отправит свой MAC исходному хосту. Компьютер «инсайдер» выполняет подмену кэша ARP таблицы, выдавая себя за легитимного участника обмена информацией. Таким образом, через этот компьютер проходит вся информация, которой обмениваются выбранные «компьютеры-жертвы». С использованием описанного выше типа атаки был получен пароль для удаленного административного доступа на один из серверов АГТУ.

После имитации «взлома» этого сервера обнаруженные уязвимости были оперативно ликвидированы службой ИБ.

Как показывает практика, сложность борьбы с подобными атаками в высшем учебном заведении в основном связана со следующими факторами:

- трудностью контроля за выполнением всеми структурными подразделениями правил ИБ;
- недостаточным уровнем подготовки персонала в области информационных технологий вообще и в области ИБ в частности, а также с невысокой степенью лояльности сотрудников;
- невозможностью использования «жестких» санкций за нарушения режима безопасности (как, например, это практикуется в частных компаниях);
- применением бесплатных утилит, использующих «небезопасные» протоколы удаленного администрирования (таких как telnet, rlogin и т.п.);
- большим количеством информационных систем, которые потенциально могут содержать конфиденциальную информацию, но при этом администрируются непосредственно пользователями, а не профильными службами вуза;
- недостаточным уровнем финансирования мероприятий, направленных на обеспечение ИБ.

Кроме того, особенности функционирования вуза делают проблематичным, а часто и невозможным, применение некоторых типовых и весьма эффективных средств обеспечения ИБ. Например, затруднительно обеспечить полноценный пропускной режим, невозможно полностью ограничить физический доступ в помещения, в которых обрабатывается конфиденциальная информация, сложно физически разграничить различные автоматизированные подсистемы, функционирующие в рамках общей автоматизированной системы управления вузом и т.д.

Оценка адекватности разработанной НКМ. Оценка уровня повреждений сервисов безопасности после реализации совокупности техногенных, природных и антропогенных угроз была произведена по методике, изложенной в [4]. Данные по оценке уровня сервисов ИБ в результате тестирования вместе с полученными с помощью предложенной модели теоретическими значениями приведены в табл. 2.

Таблица 2

Оценка уровня сервисов безопасности АГТУ

Сервис безопасности	Экспериментальная оценка / $\Omega_Э$	Расчетная оценка / $\Omega_Р$	Отклонение Ω ($\Omega_Э$-$\Omega_Р$)
Конфиденциальность	ВС / 1	ВС / 0,79	0,21
Целостность	НС / 1	НС / 0,81	0,19
Доступность	НС / 1	НС / 0,94	0,06

Отклонения индексов схожести теоретически рассчитанных и полученных в результате тестирования результатов не превышают 0,21 (среднее отклонение 0,15), что для данного типа моделей, описывающих плохо формализуемые слабо структурированные процессы, можно считать вполне допустимым. Иными словами, предложенная НКМ достаточно адекватно отражает действительность.

В результате проведенного на основе данной модели анализа были выявлены факторы, оказывающие наибольшее влияние на снижение безопасности информационных активов вуза, и даны рекомендации по повышению уровня ИБ.

Реализация указанных мер позволила поднять оценку сервиса безопасности «Доступность» до уровня «Средний», а сервиса «Целостность» до уровня «Выше среднего».

Заключение. На основании всего вышеизложенного можно сделать следующие выводы.

1. Предложенная нечеткая когнитивная модель дает возможность, последовательно пройдя все уровни ее иерархии и применяя для свертки параметров приведенные в работе формулы, оценить уровень безопасности информационных активов вуза и выработать рекомендации по его повышению. При этом использование модели позволяет более целенаправленно проводить поиск возможных уязвимостей системы ЗИ, а также аккумулировать полученные при этом знания. Данная модель применима для оценки уровня ИБ любого вуза.

2. Проверка адекватности разработанной модели показала достаточно хорошее соответствие между теоретическими результатами и данными, полученными в результате тестирования реальной системы обеспечения информационной безопасности ФГБОУ ВПО АГТУ.

Список литературы

1. Ажмухамедов И. М. Анализ и управление комплексной безопасностью на основе когнитивного моделирования / И. М. Ажмухамедов // Управление большими системами. – Москва : ИПУ РАН, 2010. – Вып. 29. – С. 5–15.

2. Ажмухамедов И. М. Динамическая нечеткая когнитивная модель влияния угроз на информационную безопасность системы / И. М. Ажмухамедов // Безопасность информационных технологий. – 2010. – № 2. – С. 68–72.

3. Ажмухамедов И. М. Методика формирования команды для реализации IT-проектов на основе нечеткой когнитивной модели оценки компетенций / И. М. Ажмухамедов, А. И. Ажмухамедов // Прикладная информатика. – 2011. – № 4 (34). – С. 70–76.

4. Ажмухамедов И. М. Оценка повреждений безопасности информационной системы на основе нечетко-когнитивного подхода / И. М. Ажмухамедов // Вопросы защиты информации. – 2012. – № 1. – С. 57–60.

5. Брумштейн Ю. М. Безопасность среды пребывания в вузах – анализ влияющих факторов и состава затрат на управление ими / Ю. М. Брумштейн, Г. Н. Бобровская, А. М. Сизов // Прикаспийский журнал: управление и высокие технологии. – 2010. – № 1 (9). – С. 83–88.

6. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. Заде. – Москва : Мир, 1976. – 165 с.

7. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. ГОСТ Р53114-2008. – Москва : Стандартинформ, 2009.

8. Защита информации. Основные термины и определения. ГОСТ Р 50922-2006. – Москва : Стандартинформ, 2006.

9. Максимов В. И. Аналитические основы применения когнитивного подхода при решении слабоструктурированных задач / В. И. Максимов, Е. К. Корноушенко // Труды ИПУ РАН. – Москва, 1999. – Т. 2.– С. 95–109.

10. Минзов А. С. Особенности комплексной информационной безопасности корпоративных сетей ВУЗов / А. С. Минзов. – Режим доступа: http://tolerance.mubiu.ru/base/Minzov(2).htm#top (дата обращения 25.12.2013). – Заглавие с экрана. – Яз. рус.

11. Недосекин А. О. Нечеткий финансовый менеджмент / А. О. Недосекин. – Москва : Аудит и финансовый анализ, 2003.

12. Поспелов Д. С. «Серые» и/или «черно-белые» [шкалы] / Д. С. Поспелов // Прикладная эргономика. Специальный выпуск «Рефлексивные процессы». – 1994. – № 1. – С. 26–39.

13. Финансовые услуги. Рекомендации по информационной безопасности. ГОСТ Р ИСО ТО 13569-2007. – Москва : Стандартинформ, 2008.

14. Egan M. The executive guide to information security,: threats, challenges, and solutions / M. Egan, T. Mather. – Symantec Press, 2005. – 288 p.

15. Kaufmann A. Introduction to Fuzzy Arithmetic: Theory and Applications / A. Kaufmann, M. Gupta. – Van Nostrand Reinhold, 1991. – 350 p.

16. Kosko B. Fuzzy cognitive maps / B. Kosko // International Journal of Man-Machine Studies. – 1986. – Vol. 1. – P. 65–75.

References

1. Azhmukhamedov I. M. Analiz i upravlenie kompleksnoy bezopasnostyu na osnove kognitivnogo modelirovaniya [Analysis and complex security management based on cognitive modeling]. *Upravlenie bolshimi sistemami* [Large systems control]. Moscow, Institute of Control Sciences of RAS, 2010, no. 29, pp. 5–15.

2. Azhmukhamedov I. M. Dinamicheskaya nechetkaya kognitivnaya model vliyaniya ugroz na informatsionnuyu bezopasnost sistemy [Dynamic fuzzy cognitive model of the effect of threats on system information security]. *Bezopasnost informatsionnykh tekhnologiy* [Information Technology Safety], 2010, no. 2, pp. 68–72.

3. Azhmukhamedov I. M., Azhmukhamedov A. I. Metodika formirovaniya komandy dlya realizatsii IT-proektov na osnove nechetkoy kognitivnoy modeli otsenki kompetentsiy [Technique of forming a team for the implementation of IT projects based on fuzzy cognitive model of competence assessment]. *Prikladnaya informatika.* [Applied Informatics], 2011, no. 4 (34), pp. 70–76.

4. Azhmukhamedov I. M. Otsenka povrezhdeniy bezopasnosti informatsionnoy sistemy na osnove nechetko-kognitivnogo podkhoda [Damage assessment information system security based on fuzzy cognitive approach]. *Voprosy zashchity informatsii* [Journal of Data Protection], 2012, no. 1, pp. 57–60.

5. Brumshteyn Yu. M., Bobrovskaya G. N., Sizov A. M. Bezopasnost sredy prebyvaniya v vuzakh – analiz vliyayushchikh faktorov i sostava zatrat na upravlenie imi [Security of stay environment in universities – analysis of influencing factors and costs of their management]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii.* [Caspian Journal: Management and High Technologies], 2010, no. 1 (9), pp. 83–88.

6. Zade L. *Ponyatie lingvisticheskoy peremennoy i ego primenenie k prinyatiyu priblizhennykh resheniy* [Concept of linguistic variable and its application to the adoption of approximate solutions]. Moscow, Mir, 1976. 165 p.

7. Data protection. Ensuring information security in the organization. Basic terms and definitions. GOST R53114-2008. Moscow, Standartinform, 2009. (In Russ.)

8. Data protection. Basic terms and definitions. GOST R 50922-2006. Moscow, Standartinform, 2006. (In Russ.)

9. Maksimov V. I., Kornoushenko Ye. K. Analiticheskie osnovy primeneniya kognitivnogo podkhoda pri reshenii slabostrukturirovannykh zadach [Analytical bases for the use of the cognitive approach

in solving semistructured problems]. *Trudy Instituta problem upravleniya RAN* [Proceedings of Institute of Control Sciences of RAS]. Moscow, 1999, no. 2, pp. 95–109.

10. Minzov A. S. *Osobennosti kompleksnoy informatsionnoy bezopasnosti korporativnykh setey VUZov* [Features of complex information security of corporate networks of universities]. Available at: http://tolerance.mubiu.ru/base/Minzov(2).htm#top (accessed 25 December 2013).

11. Nedosekin A. O. *Nechetkiy finansovyy menedzhment* [Fuzzy financial management]. Moscow, Audit and Financial Analysis, 2003.

12. Pospelov D. S. «Serye» i/ili «cherno-belye» [shkaly] ["Grey" and/or "black and white" scales]. *Prikladnaya ergonomika. Spetsialnyy vypusk «Refleksivnye protsessy»* [Applied Ergonomics. Special Issue "Reflexive Processes"], 1994, no. 1, pp. 26–39.

13. Financial services. Recommendations for information security. GOST R ISO TO 13569-2007. Moscow, Standartinform, 2008.

14. Egan M., Mather T. *Executive guide to information security, the: threats, challenges, and solutions.* Symantec Press, 2005. 288 p.

15. Kaufmann A., Gupta M. Introduction to Fuzzy Arithmetic: Theory and Applications. Van Nostrand Reinhold, 1991. 350 p.

16. Kosko B. Fuzzy cognitive maps. *International Journal of Man-Machine Studies*, 1986, no. 1, pp. 65–75.