УДК 378:004.02

НЕОБХОДИМОСТЬ ПРЕПОДАВАНИЯ БИОМЕТРИЧЕСКИХ МЕТОДОВ В УЧЕБНОМ КУРСЕ «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

Белова Е.П.

ГОУ ВПО «Уфимский государственный авиационный технический университет», Уфа, e-mail: super.yelenar@yandex.ru

Проведён анализ требований, предъявляемых к студентам в ходе прохождения учебного курса «Управление информационной безопасностью». Представлены принципы разработки и функционирования систем управления информационной безопасностью. Приведён перечень задач, на решение которых и направлено управление информационной безопасностью. Рассмотрены задачи, которые должны уметь решать будущие специалисты в области информационной безопасности. Проведён анализ цели и задач, которые должен решить студент в ходе прохождения учебного курса «Управление информационной безопасностью». Приведена классификация методов защиты информации, применимая для каждой компании или предприятия, оснащённого информационной системой. Проанализировано место биометрических методов обеспечения информационной безопасности среди средств защиты информации. Представлен перечень областей, в которых их роль возрастает быстрыми темпами. Рассмотрены распространённые классификации биометрических методов защиты информации. Выявлена их возрастающая роль в системе управления информационной безопасностью по сравнению с традиционными методами защиты информации. Рассмотрена перспектива увеличения количества учебной нагрузки касательно биометрических методов обеспечения информационной безопасности в составе лекционных и лабораторных занятий по дисциплине «Управление информационной безопасностью», исходя из требований, предъявляемых к составу данного учебного курса и проведению лекционных и лабораторных занятий.

Ключевые слова: управление информационной безопасностью, система управления информационной безопасностью, информационная безопасность, учебный курс, дисциплина, защита информации, биометрические методы защиты информации, биометрические методы обеспечения информационной безопасности, лекция, лабораторное занятие

THE NEED FOR TEACHING BIOMETRIC METHODS IN THE EDUCATIONAL COURSE «INFORMATION SECURITY MANAGEMENT»

Belova E.P.

Ufa State Aviation Technical University, Ufa, e-mail: super.yelenar@yandex.ru

The analysis of the requirements for students during the course «Information Security Management» was conducted. The principles of development and operation of information security management systems are presented. The list of tasks that are addressed and management of information security. The tasks that should be addressed by future specialists in the field of information security are considered. An analysis of the goals and objectives that the student must solve during the course «Information Security Management». A classification of information protection methods applicable for each company or enterprise equipped with an information system is given. The place of biometric methods of ensuring information security among the means of information protection is analyzed. A list of areas in which their role is increasing rapidly is presented. Considered common classification of biometric methods of information protection. Their increasing role in the information security management system as compared with traditional methods of information protection is revealed. Considered the prospect of increasing the amount of training load on biometric methods of ensuring information security in the composition of lectures and laboratory classes in the discipline «Information Security Management», based on the requirements for the composition of this training course and its lectures and laboratory classes.

Keywords: information security management, information security management system, information security, training course, discipline, information protection, biometric information protection methods, biometric information security methods, lecture, laboratory lesson

Экономическая ситуация на рынке труда XXI в. «требует высококвалифицированных специалистов в области информационных технологий. Доступные на рынке труда вакансии стараются покрыть полный жизненный цикл процесса разработки программного обеспечения – начиная с процесса предложения различных вариантов и заканчивая их технической поддержкой. И на каждом этапе требуется хорошо обученный персонал. Таким образом, можно утверждать, что современные работодатели ждут от будущих сотрудников высокого профессионального уровня, знания новейших решений технологических, управленческих и коммуникационных проблем» [1, с. 54]. Управление информационной безопасностью – важный аспект в подготовке высококвалифицированных специалистов, способных обеспечить оптимальную информационную защиту на предприятии, на котором они работают.

Управление информационной безопасностью реализуется при помощи систем

управления информационной безопасности (СУИБ), которые представлены целым комплексом решений по обеспечению информационной безопасности предприятия. Задачи студентов, усваивающих данный учебный курс, – в совершенстве владеть профессиональной терминологией, знать теоретическую базу изучаемого предмета, уметь администрировать СУИБ, своевременно корректировать её работу и комплектовать её из разнозадачных программных продуктов. «Переход к новому технологическому укладу будут совершать специалисты в области работ с большими данными, интеллектуального анализа и принятия решений, машинного обучения, технологий виртуальной реальности и решения задач с помощью машинного зрения» [2, с. 170].

В ходе прохождения курса «Управление информационной безопасностью» студенты взаимодействуют с различным инструментарием. Однако необходимо учитывать, что некоторые инструменты, направленные на обеспечение информационной безопасности, могут основываться на биометрических данных человека, то есть быть биометрическими. Биометрические методы обеспечения информационной безопасности применяются сравнительно недавно и им пока не уделяется время на лабораторных работах.

В рамках данной статьи рассматриваются основы учебного курса «Управление информационной безопасностью» и возможности изучения биометрических инструментов в рамках данного предмета.

Цель исследования: обосновать целесообразность увеличения времени преподавания биометрических методов защиты информации в учебном курсе «Управление информационной безопасностью».

Материалы и методы исследования

Управление информационной безопасностью (Information security management, ISM) представляет собой циклический процесс, который в обязательном порядке должен включать:

− определение необходимой степени защиты информации;

− постановку задач;

− проведение сбора и анализа данных о текущем состоянии информационной безопасности на заданном предприятии;

− оценку информационных рисков;

− разработку плана мероприятий, направленных на выявление и ликвидацию угроз информационной безопасности предприятия;

− разработку плана мероприятий, направленных на минимизацию последствий после наступления ситуации, в ходе которой был нанесён ущерб из-за нарушения информационной безопасности заданного предприятия;

− реализацию и внедрение механизмов контроля;

− распределение ролей и ответственности между сотрудниками предприятия, направленных на уменьшение вероятности реализации угроз и минимизацию ущерба, в случае нарушения информационной безопасности;

− обучение персонала основным правилам информационной безопасности, принятым на данном предприятии;

− повышение мотивации персонала в соблюдении принятых руководством предприятия мер относительно информационной безопасности предприятия;

− оперативную работу по реализации защитных мер;

− мониторинг функционирования механизмов контроля, корректировка их работы в случае необходимости [3].

Тем самым система управления информационной безопасностью (СУИБ) является неотъемлемой частью любого предприятия. Её разработка и функционирование базируются на следующих принципах:

− комплексном подходе – СУИБ должна охватывать всю информационную систему предприятия;

− обеспечении стратегии заданного предприятия;

− непрерывности самого процесса управления;

− понятности и доступности в управлении;

− рациональном балансе всех важных показателей, к которым, как правило, относят ключевые функции системы относительно стратегии предприятия, её производительность и издержки, непосредственно связанные с её работой;

− процессном подходе (все процессы функционирования СУИБ представляют собой замкнутый цикл) [4].

Студент в ходе прохождения учебного курса «Управление информационной безопасностью» должен приобрести навыки администрирования систем управления информационной безопасностью, то есть уметь:

− составлять план по реализации мер, направленных на обеспечение информационной безопасности информационной системы заданного предприятия;

− непосредственно участвовать в организации комплекса мероприятий, направленных на усиление информационной безопасности предприятия и ликвидацию последствий, если информационный урон уже был нанесён;

− генерировать действенные предложения, позволяющие усовершенствовать работу СУИБ;

– вести разработку подсистемы управления информационной безопасностью [5].

Методы защиты любого предприятия включают в себя такие средства, как:

– технические;
– физические;
– юридические;
– административные [6].

Для эффективного функционирования системы управления информационной безопасностью предприятия должен соблюдаться системный подход, то есть все виды средств защиты информации должны использоваться одновременно и управляться централизованно [6].

Технические средства включают:

– системы шифрования и дешифрования информации;
– системы разграничения полномочий и управления доступом;
– антивирусное программное обеспечение;
– прокси-серверы;
– сетевые экраны;
– сети VPN на основе шифрования;
– защищённый канал IPSec и его протоколы [6].

Биометрические методы защиты информации нашли своё применение именно в системах разграничения полномочий и управления доступом.

На сегодняшний день они широко используются в следующих отраслях:

– системе паспортного контроля (паспортах нового поколения);
– системе визового контроля;
– сопровождении авиапассажиров;
– контрольно-пропускной системе;
– входе на электронное рабочее место;
– удалённом доступе к банковским операциям [7, 8].

Некоторые биометрические параметры могут изменяться под воздействием эмоций, заболевания, возрастных изменений, другие – остаются неизменными. Биометрические параметры, подверженные изменениям, называются динамическими, а неизменные – статическими [7].

Таким образом, к статическим параметрам относятся:

– термограмма лица;
– форма лица;
– радужная оболочка глаза;
– сетчатка глаза;
– отпечаток пальца;
– термограмма кисти руки;
– код ДНК [7].

Динамические параметры же включают в себя:

– речевые параметры;
– почерк;
– клавиатурный почерк [7].

По использованной технологии биометрические методы разделяют на:

– оптоэлектронные;
– полупроводниковые;
– тепловизионные;
– телевизионные;
– ультразвуковые;
– электрооптические;
– пироэлектрические;
– комбинированные [7].

Распространена и другая классификация биометрических параметров. По ней они делятся на:

– случайно приобретённые;
– генотипные;
– поведенческие [8].

Случайно приобретённые включают в себя:

– радужную оболочку глаза;
– сетчатку глаза;
– отпечаток пальца;
– строение кровеносной системы [8].

К генотипным параметрам относят:

– геометрию лица;
– геометрию руки;
– ДНК;
– речевые параметры [8].

Поведенческие параметры представлены:

– почерком;
– клавиатурным почерком [8].

Достоинствами биометрических методов аутентификации и идентификации являются высокая эффективность и комфортность применения [8, 9].

Однако у данных инструментов есть и недостатки. Они связаны с особенностями самого инструмента. Например, сканеры отпечатков пальцев склонны к загрязнениям, а системы распознавания по геометрии лица требуют определённого положения лица перед сканером [8].

Таким образом, биометрические средства защиты информации применяются для разграничения полномочий и управления доступом в системах управления информационной безопасностью.

Результаты исследования и их обсуждение

Учебный курс «Управление информационной безопасностью» представлен лекционными и лабораторными занятиями.

Биометрические инструменты защиты информации широко используются в системах аутентификации и идентификации. Так как в последнее время их количество растёт и многие отрасли активно их используют, то целесообразно изучать их в рамках дисциплины «Управление информационной безопасностью».

Лекционные занятия знакомят студентов с основной терминологией, наиболее

распространёнными средствами защиты информации и принципами их работы, основными принципами администрирования систем управления информационной безопасностью. Поэтому в рамках данной дисциплины на лекционных занятиях важно знакомить студентов с биометрическими средствами защиты информации.

В рамках лабораторных работ студенты должны научиться:

– выбирать лучший вариант средства защиты информации, зарегистрированный в Государственном реестре сертифицированных средств защиты информации;

– синтезировать средства защиты информации, зарегистрированные в Государственном реестре сертифицированных средств защиты информации, в набор наиболее рациональным вариантом;

– выбирать лучший вариант реагирования на события нарушения информационной безопасности;

– выбирать систему управления информационной безопасностью, подходящую для определённого предприятия [5].

В условиях непрерывного роста биометрических технологий биометрические средства защиты информации должны рассматриваться в рамках этих умений и быть включёнными в перечень средств, рассматриваемых на лабораторных работах.

Тем самым биометрические средства защиты информации рекомендуются к изучению в ходе учебного курса «Управление информационной безопасностью».

Заключение

«Внедрение компетентностного подхода в высшее профессиональное образование привело к изменениям в его содержании, методах и формах подготовки. Вузовское обучение сегодня носит комплексный, междисциплинарный характер и ориентировано на овладение не только знаниями и умениями, но и на способность их использовать в профессиональной деятельности» [1, с. 54]. На сегодняшний день биометрические средства защиты информации охватывают практически все отрасли России. Высокая эффективность и удобство использования данных инструментов позволяет с успехом применять их в системах разграничения полномочий и управления доступом в учреждениях различного уровня. Поэтому целесообразно включить изучение биометрических технологий в учебный курс «Управление информационной безопасностью».

Список литературы

1. Иванова А.Д., Бармина О.В. Анализ личностных и профессиональных требований, предъявляемых к подготовке системного аналитика // Научное обозрение. Педагогические науки. 2017. № 2. С. 54–59.

2. Лакман И.А., Иванова А.Д., Муругова О.В. Методическое обеспечение педагогической практики аспирантов технических и экономических направлений // Современные наукоемкие технологии. 2018. № 4. С. 169–173.

3. Понятие системы управления информационной безопасностью. GlobalTrust Solutions [Электронный ресурс]. URL: http://globaltrust.ru/ru/uslugi/vnedrenie-sistem-upravleniya-informacionnoi-bezopasnostyu/ponyatie-sistemy-upravleniya-informacionnoi-bezopasnostyu (дата обращения: 7.11.2018).

4. AR система управления информационной безопасностью ARinteg [Электронный ресурс]. URL: https://www.arinteg.ru/articles/upravlenie-informatsionnoy-bezopasnostyu-26728.html (дата обращения: 9.11.2018).

5. Гузаиров М.Б., Машкина И.В. Управление защитой информации на основе интеллектуальных технологий: учеб. пособие. М.: Машиностроение, 2013. 241 с.

6. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 4-е изд. СПб.: Питер, 2010. 944 с.

7. Биометрические системы – надёжная защита информации [Электронный ресурс]. URL: https://umniedoma.ru/biometricheskie-sistemy-nadezhnaya-zashhita-informacii/ (дата обращения: 10.11.2018).

8. Загинайло М.В., Каплун В.В. Преимущества и недостатки применения биометрических систем в информационной безопасности // Молодой ученый. 2016. № 30. С. 73–75 [Электронный ресурс]. URL https://moluch.ru/archive/134/37550/ (дата обращения: 10.11.2018).

9. Швырев Б.А. Информационная безопасность и биометрия // Вестник института: преступление, наказание, исправление. 2015. № 2 (30). С. 87–89.