УДК 378.14
DOI: http://dx.doi.org/10.21686/1818-4243-2021-3-36-45

В.А. Сизов[1], Д.М. Малиничев[2], Х.Х. Кучмезов[3], В.В. Мочалов[2]

[1] Российский экономический университет им. Г.В. Плеханова, Москва, Россия
[2] Негосударственное образовательное частное учреждение высшего образования «Московский финансово-промышленный университет «Синергия», Москва, Россия
[3] Финансовый университет при Правительстве Российской Федерации, Москва, Россия

Применение метода проблемного обучения в изучении дисциплины «Информационная безопасность»

Целью настоящей статьи *является развитие у студентов критического мышления для решения задач в области информационной безопасности за счет использования метода проблемного обучения в преподавании дисциплины «Информационная безопасность». Подчеркивается место данного метода в развитии критического мышления, исследовательской креативности студентов и достижений ими лучшего понимания учебного материала в области информационной безопасности.*

Материалы и методы исследования. *Методом анализа предметной области выделены главные условия эффективности проблемного обучения в изучении дисциплины «Информационная безопасность»: мотивация студентов, посильность и значимость предлагаемых студентам проблемных ситуаций по различным аспектам информационной безопасности, диалогическое доброжелательное общение преподавателя со студентами. В качестве материалов исследования рассматривается пример использования метода проблемного обучения в решении задачи защиты информации в государственных информационных системах (ГИС) с устройствами терминального доступа. В примере представлена проблема повышения эффективности защиты информации в ГИС с устройствами терминального доступа, т.е. ГИС, использующих архитектуру «тонкого клиента», а также предложен способ ее решения за счет оценки угроз и совершенствования соответствующих механизмов обеспечения информационной безопасности, представленных в нормативно-правовых документах, регламентирующих требования по защите информации в ГИС с устройствами терминального доступа.*

Результаты. *В работе рассмотрена практическая задача создания и разрешения проблемной ситуации по защите информации в ГИС с устройствами терминального доступа, которую можно использовать в учебном процессе для решения аналогичных задач методом проблемного обучения.*

Создание проблемной ситуации основано на имеющихся противоречиях в нормативно-правовых актах, регулирующих функционирование и защиту информации такого типа систем, в которых защищаемая информация обрабатывается в целях исполнения законодательства и обеспечения функционирования органов власти. В результате использования системного подхода, предполагающего рассмотрение процесса защиты информации в виде совокупности этапов формирования требований к ГИС, использующих архитектуру «тонкого клиента», совершенствования нормативно-правовой базы, обучаемые формируют предложения по защите информации в ГИС, использующих архитектуру «тонкого клиента» для обеспечения проектной защищенности ГИС, учитывающие комплекс актуальных угроз безопасности информации.

Представленное разрешение проблемной ситуации в рассмотренной задаче требует от обучаемых общекультурных компетенций, таких как: выявление противоречий, сталкивание противоположных точек зрения, сопоставление фактов, рассмотрение проблемы с разных точек зрения, обобщение, конкретизация фактов и т. д.

Выводы. *Таким образом, в работе обоснован метод проблемного обучения в изучении дисциплины «Информационная безопасность» и представлен пример его использования в решении задачи защиты информации в ГИС с устройствами терминального доступа. В результате обучаемые должны выявить угрозы, отсутствующие в банке данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России) и определить направления дальнейшего развития обеспечения информационной безопасности и защиты информации в ГИС с устройствами терминального доступа. Практическое решение этой задачи группой студентов в рамках изучения дисциплины «Информационная безопасность» показало высокий уровень освоения компетенций.*

Ключевые слова: *метод проблемного обучения, методика преподавания, государственные информационные системы, информационная безопасность, устройства терминального доступа, угрозы информационной безопасности*

Valery A. Sizov[1], Dmitry M. Malinichev[2], Khamzat K. Kuchmezov[3], Vadim V. Mochalov[2]

[1] Plekhanov Russian University of Economics, Moscow, Russia
[2] Non-state educational private institution of higher education “Moscow Financial and Industrial University “Synergy”, Moscow, Russia
[3] Financial University under the Government of the Russian Federation, Moscow, Russia

Application of the Method of Problem Learning in the Study of the Discipline “Information Security”

The purpose of this article *is to develop students’ critical thinking for solving problems in the field of information security by using the method of problem learning in teaching the discipline “Information Security”. The role of this method in the development of critical thinking, research creativity of students and their achievement of a better understanding of educational material in the field of information security is emphasized.*

Materials and research methods. *The main conditions for the effectiveness of problem learning in the study of the discipline “Information Security” are highlighted by the method of analysis of the*

subject area: motivation of students, the feasibility and significance of problem situations offered to students on various aspects of information security, dialogical friendly communication between lecturer and students. As research materials, an example of using the method of problem learning in solving the task of information protection in state information systems with terminal access devices is considered. The example presents the problem of increasing the efficiency of information protection in state information systems with terminal access devices, i.e. state information systems using the "thin client" architecture, as well as a way to solve it by assessing threats and improving the relevant mechanisms for ensuring information security, presented in the regulatory documents governing the requirements for information protection in state information systems with terminal access devices.

Results. *The paper considers the practical task of creating and resolving a problem situation for the protection of information in state information systems with terminal access devices, which can be used in the educational process to solve similar tasks by the method of problem learning.*

The creation of a problematic situation is based on the existing contradictions in the regulations governing the functioning and protection of information of this type of systems in which the protected information is processed in order to comply with legislation and ensure the functioning of authorities. As a result of using a systematic approach, which involves considering the process of information protection in the form of a set of stages in the formation of requirements for state information systems using the architecture of the "thin client", improving the regulatory framework, the trainees form proposals for the protection of information in state information systems using the architecture of the "thin client" to ensure the design security of state information systems, taking into account the complex of urgent threats to information security. The presented solution to the problem situation in the considered task requires from the trainees general cultural competencies, such as: identifying contradictions, colliding opposing points of view, comparing facts, considering the problem from different points of view, generalizing, concretizing facts, etc.

Conclusions. *Thus, the paper substantiates the method of problem learning in the study of the discipline "Information Security" and presents an example of its use in solving the problem of information protection in state information systems with terminal access devices. As a result, the trainees must identify threats that are absent in the information security threat databank of the Federal Service for Technical and Export Control of the Russian Federation (FSTEC of Russia) and determine the directions for further development of information security and information protection in state information systems with terminal access devices. The practical solution of this problem by a group of students within the framework of the study of the discipline "Information Security" showed a high level of competence development.*

Keywords: *problem learning method, teaching methodology, state information systems, information security, terminal access devices, threats to information security.*

Введение

Проблемно-ориентированное обучение – это идеология, педагогическая стратегия, особый стиль постижения знаний, при котором возможным становится полноценное овладение проблемой с глубоким, активным, стойким освоением материала реальных жизненных ситуаций [1].

Проблемно-ориентированные методы обучения широко применяются в образовательных контекстах для развития критического мышления и решения проблем в реальных учебных ситуациях [2]. Тесная связь метода проблемного обучения с производственным сотрудничеством и междисциплинарным обучением способствовала его распространению за пределы традиционной области образования в прикладные дисциплины, такие как технические науки [3], в том числе, в области информационной безопасности.

Проблемно-ориентированный подход к обучению позволяет сфокусировать внимание студентов на анализе и разрешении какой-либо конкретной проблемной ситуации, что становится отправной точкой в процессе обучения. При этом иногда важно не столько решить проблему, сколько грамотно ее поставить и сформулировать. Проблемная ситуация максимально мотивирует студентов осознанно получать знания, необходимые для ее решения. Междисциплинарный подход к обучению позволяет научить студентов самостоятельно «добывать» знания из разных областей, группировать их и концентрировать в контексте конкретной решаемой задачи [4].

В данной статье рассматривается применение метода проблемного обучения в изучении дисциплины «Информационная безопасность». Проблемное обучение рассматривается как эффективный метод, с помощью которого студентам может быть оказана помощь в приобретении базовых компетенций в области информационной безопасности.

Способ решения учебных задач в изучении дисциплины «Информационная безопасность» предполагает, прежде всего, что студенты должны идентифицировать и определять проблему, овладевать конкретными исследовательскими методами процесса решения (алгоритмическими и эвристическими стратегиями) и, в то же время, уметь аргументировать свою точку зрения. С этой целью в качестве примера в статье разрабатывается задача создания и разрешения проблемной ситуации по защите информации в ГИС с устройствами терминального доступа. Рассмотренный пример может быть использован при решении аналогичных учебных задач.

1. Обоснование эффективности проблемного обучения в изучении дисциплины «Информационная безопасность»

Основным элементом современной системы образования является проблемное обучение, которое решает основные задачи современного обучения, в том числе и применение метода проблемного обучения.

Однако на сегодняшний день педагогический процесс не в полной степени ориентирован на проблемное обучение как средство активизации мыслительной деятельности обучающихся. Система совре-

менного образования страдает тем, что культивирует фрагменты знания, использует традиционный объяснительно-иллюстративный метод [3]. Усиливается противоречие между имеющимися научными разработками по активизации мыслительной деятельности средствами проблемного обучения и невостребованностью их в практической деятельности [16].

Проблемное обучение появилось как результат достижения передовой практики и теории обучения в сочетании с традиционным типом обучения и является эффективным средством для технического обучения и интеллектуального развития обучающихся.

Исторический развитие проблемного обучения начинается с введения так называемого исследовательского метода, которые были разработаны Джоном Дьюи. Глубокие исследования в области проблемного обучения начались в 60-х годах [5]. Разработка способов возбуждения мыслительной деятельности студентов привела во второй половине 19 и начале 20 века к внедрению в преподавание таких учебных дисциплин как: опытно-эристического (А.Л. Герд), лабораторно-эвристического (Ф.А. Винтергальтер), метода лабораторных уроков (К.П. Ягодский) и других методов, которые в силу специфики их существа заменил термином «исследовательский метод» [20]. В 20 веке идеи проблемного обучения получили мощное импульс к развитию и распространение в образовательной практике.

Наибольшее влияние на развитие современной концепции проблемного обучения оказала работа Дж. Брунера («Процесса обучения», 1960). В ее основе лежат идеи инструктирование учебного материала и доминирующей роли интуитивного мышления в процессе усвоения новых знаний как основы эвристического мышления. С этого периода в литературе настойчиво стали развивается мысль о необходимости усиления роли исследовательского метода в обучении техническим дисциплинам [6]. Проблемность в обучении рассматривалась как одна из закономерностей умственной деятельности учащихся.

Обучение студентов навыкам решения проблем должно включать: получение новых знаний по дисциплине «Информационная безопасность» через решение проблем; решать задачи, возникающие в процессе обучения; применение и адаптацию различных подходящих стратегий для решения проблем; наблюдение и критический анализ процесса решения задач в области информационной безопасности. Проблемное обучение — это система методов обучения, при которой студент получает знания не путем заучивания и запоминания их в готовом виде, а в результате мыслительной работы по решению проблем и проблемных задач, построенных на содержании изучаемого материала.

Одним из наиболее важных этапов проблемного обучения является этап постановки проблемы [17]. В реализации данного этапа и эффективном решении его учебных задач на занятиях по информационной безопасности педагоги использовать следующие пути постановки учебной проблемы: – создание проблемной ситуации; – использование приемов подводящего диалога или побуждающего диалога; – использование мотивирующих приемов. Сама по себе способность решать проблемы базируется на ряде этапов: понимание проблемы, планирование решения проблемы, решение проблемы согласно разработанного плана.

При этом необходимо оценить результативность использования метода проблемного обучения при изучении дисциплины «Информационная безопасность» в образовательном процессе. Для определения эффективности реализации современных методов обучения можно воспользоваться рядом критериев.

Критерий № 1. Способность обучающихся действовать в условиях проблемной ситуации. Показатель – уровень, на котором обучающийся обнаруживает проблему и может ли обучающийся найти путь решения возникшей проблемы.

Критерий № 2. Активность и отвлекаемость обучающихся. Показатель – самостоятельность в выполнении заданий (после получения пояснения к заданию) и отвлекаемость (наличие любых действий, не связанных с обучением).

Критерий № 3. Отношение обучающихся к учебному процессу. Показатели – эмоциональное отношение студентов к обучению и отношение обучающихся к возникающим трудностям до применения метода проблемного обучения.

Эффективность применения технологии проблемного обучения в преподавании дисциплины «Информационная безопасность» может быть оценена по таким параметрам, как информативность учебного материала, используемого для изучения дисциплины, актуальность и значимость материалов для подготовки, технологическая культура преподавателя и применение современных информационных технологий в процессе обучения. Результативность образовательного процесса следует в первую очередь оценивать, по основным навыкам, умениями и компетенциям, которые формируются у обучающихся в их учебно-познавательной деятельности в области информационной безопасности. Полнота и степень соответствия обозначенным показателям будут свидетельствовать об

эффективности применения метода проблемного обучения в изучении дисциплины «Информационная безопасность».

Как пример проблемы, предлагаемой для решения студентами в ходе учебного процесса, предлагается рассмотреть защиту информации в ГИС с устройствами терминального доступа.

2. Разработка задачи создания и разрешения проблемной ситуации по защите информации в государственных информационных системах с устройствами терминального доступа.

2.1. Обоснование актуальности проблемы защиты информации в государственных информационных системах с устройствами терминального доступа

В настоящее время в области информационной безопасности актуальны задачи, связанные с защитой информации в ГИС [22]. Особую сложность при решении этих задач представляют меры защиты информации, которые нечетко описаны и не имеют описанных угроз в банке данных ФСТЭК России. Одной из таких мер является использование устройств терминального доступа для обработки информации [21]. Несмотря на то, что данная мера не обязательна к применению ни в одном из классов ГИС, она получила широкое распространение в связи с потенциально более дешевой реализацией, простой эксплуатацией, а также возможностью масштабируемости. Применение этой меры позволяет сосредоточить все ресурсы на серверной части и удешевить клиентские устройства, которым больше нет необходимости хранить и обрабатывать информацию, а лишь получать и передавать её между сервером и терминалом-клиентом [7]. Это позволяет динамически менять число подключенных терминалов, подключая новые и отключая уже подключенные ранее. Появляется возможность менять вышедшие из строя терминалы на исправные без необходимости восстановления хранившейся информации, настроек и параметров. Сосредоточение информации в одном месте делает сервер более привлекательным для злоумышленников с целью нарушений конфиденциальности, целостности или доступности информации. Сложность представляет также физическая защита терминалов, безопасность сетевого взаимодействия терминалов-клиентов с сервером, определение принадлежности терминалов к организации или органу исполнительной власти и их идентификация, наличие программных закладок и недекларированных возможностей. Следует определить и функции, которые необходимо выполнять терминалу-клиенту и терминальному серверу. В частности, для системы автоматизации медицинской и административной деятельности единой ГИС в сфере здравоохранения определены функции [8], приведенные в таблице 1.

Анализ таблицы 1 показывает, что для терминального сервера требуется обеспечение возможности вывода информации на сетевые принтеры, съемные носители информации (USB-накопители), системы трансляции звука. Необходимо также обеспечить

Таблица 1

Требования к терминальному серверу

Table 1

Requirements for the terminal server

Наименование показателя, ед. изм. показателя	Описание, значение
Назначение программного обеспечения	Программное обеспечение терминального доступа
Функция параллельного подключения к существующей сессии с возможностью просмотра и взаимодействия с системой	Наличие
Возможность трансляции принтера в сессию средствами клиента	Наличие
Возможность трансляции локального каталога в сессию средствами клиента	Наличие
Возможность трансляции USB-накопителей в сессию средствами клиента	Наличие
Возможность трансляции звука в сессию средствами клиента	Наличие
Функция запуска удалённого приложения без загрузки рабочего окружения сервера	Наличие
Обеспечение информационной среды для работы пользователя с тонкого клиента на базе Linux	Наличие
Клиент терминального доступа/доступа к виртуальным рабочим столам для операционной системы (linux)	Наличие
Клиент терминального доступа	Наличие
Распределение и контроль прав доступа пользователей к информационным ресурсам	Наличие
Централизованное управление списками пользователей	Наличие
Возможность аутентификации пользователей по паре логин\пароль	Наличие
Транспортный протокол передачи данных совместим с протоколом Nomachine NX	Наличие
Возможность балансировки нагрузки через разделение запросов клиентов на группу серверов	Наличие
Возможность «заморозки» рабочих окружений клиентов и восстановление работы с исходной точки через некоторое время	Наличие

возможность трансляции локального каталога в сессию средствами клиента, а значит, присутствует необходимость в долговременном хранилище информации на стороне клиента. Имеются требования в централизованном управлении доступом, распределении и контроле прав доступом клиентов, обеспечение подключения терминалов с различными операционными системами. Каждое из этих требований накладывает свои сложности и ограничения. В настоящий момент на рынке имеются программно-аппаратные и программные продукты, способные удовлетворить данные требования [9].

Отсутствие угроз для терминальных устройств в банке данных ФСТЭК России, нечеткое определение терминального устройства в документах ФСТЭК России [21], в частности, отсутствие определения допустимых количественных характеристик терминальных устройств, описания конкретных механизмов по ограничению функционала хранения и обработки информации, отсутствие требований для терминальных устройств и системы их сертификации, не позволяют выработать единый подход к построению защищенной терминальной системы ГИС.

2.2 Разрешение проблемной ситуации на основе исследования модели тонких клиентов государственной информационной системы и взаимодействия сервера с тонкими клиентами

Для разрешения проблемной ситуации целесообразно использовать клиент-серверную модель взаимодействия сервера с тонкими клиентами ГИС. Терминальную модель ГИС можно представить, как совокупность терминального сервера, терминалов-клиентов, каналов связи, сетевых устройств и протоколов их

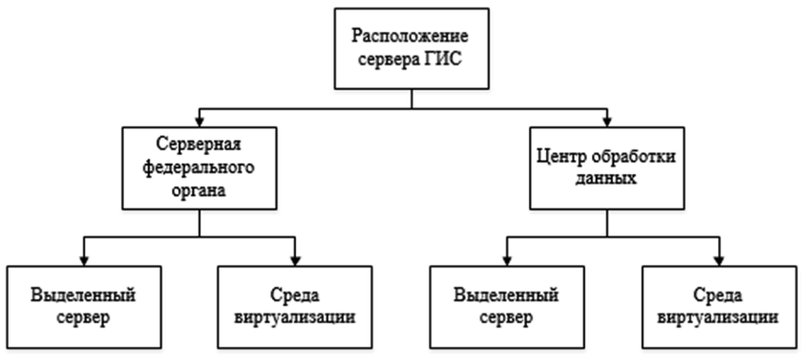

Рис. 1. Способы реализации терминального сервера

Fig. 1. Ways to implement a terminal server

взаимодействия. В зависимости от масштаба ГИС, её распределённости и вовлеченных в её функционирование лиц и органов исполнительной власти, напрямую зависит организация обеспечения её работы и функционирования. Защищенность ГИС зависит от многих факторов, как наличие выходов в сети общего пользования, территориальное размещение, объём и характер обрабатываемых сведений [13]. Поэтому при описании модели терминального доступа к ГИС необходимо учитывать многие факторы.

По физическому расположению терминального сервера ГИС можно выделить два основных места: серверная комната федерального органа исполнительной власти и центр обработки (хранения) данных (рисунок 1). В первом случае задача обслуживания терминального сервера целиком ложится на орган федеральной власти, который должен обеспечить помещения, обслуживающий персонал, вычислительную технику и оборудование. Это возможно при относительно небольшом размере ГИС или при высоком уровне значимости обрабатываемой (хранящейся) информации. Конечно, это влечет за собой потенциально большие убытки в связи с необходимостью самостоятельно заниматься теми вещами, которые в противном случае делегировались бы центру обработки (хранению) данных [15]. Сложнее оценить необходимый вычислительный объём, необходимый для такого сервера, так как если установить более мощный сервер с запасом, то излишние мощности будут не задействованы и не востребованы, а при установке обычного или более слабого сервера есть вероятность внезапного роста необходимости вычислительных ресурсов, когда развертывание дополнительных серверов или более мощного замещающего сервера будет затруднено или невозможно в связи со сложностями переноса ГИС или особенностями помещений, в которых располагается сервер [14]. Однако, с другой стороны, в некоторых случаях такой подход, наоборот, позволяет более оперативно производить изменения, так как отсутствует необходимость согласования этих изменений с центром обработки данных. Размещение терминального сервера в центре обработки данных позволяет делегировать многие работы, связанные с обеспечением функционирования, но внесение изменений требует их согласования. Важным является надежность центра обработки данных, так как делегирование некоторых работ влечет и делегирование связанных с ними информационных рисков, управление которыми может быть недостаточно эффективным, а

последствия затронуть ГИС, федеральный орган исполнительной власти, физических и юридических лиц [10].

По логическому расположению терминальный сервер ГИС может занимать как выделенный сервер, так и часть сервера, находясь в среде виртуализации, развернутой на этом сервере [18]. Во втором случае необходимо обеспечить безопасность этой среды виртуализации, недопустимость утечки информации и внесения деструктивных воздействий со стороны основной системы и других систем среды виртуализации.

Для выполнения возложенных функций применяется протокол прикладного уровня RDP [11]. Данный протокол позволяет подключаться к удаленному рабочему столу (терминальному серверу) и взаимодействовать с ним, как с обычным рабочим столом. Это особенно удобно пользователям, так как они практически не заметят различий между персональным компьютером и тонким клиентом.

Аутентификация должна выполняться отдельно для терминала и пользователя. Аутентификация терминала позволяет установить, что доступ к терминальному серверу устанавливается с авторизованного терминала, а значит с применением физических, технических и организационных мер по защите этого терминала и канала связи. Для аутентификации и шифрования сетевого трафика могут применяться различные протоколы. Первой должна быть проведена аутентификация терминала. Для аутентификации терминала может применяться электронная подпись или протокол аутентификации на основе симметричного шифрования. Возможными протоколами сетевого взаимодействия являются:

- TLS;
- IPsec;
- SSH;
- SFTP;
- FTPS;
- SCP;
- Kerberos.

2.3 Исследование угроз информационной безопасности для модели тонких клиентов государственной информационной системы, отсутствующих в банке данных угроз ФСТЭК России

Исследование угроз информационной безопасности является неотъемлемым и необходимым этапом при разработке системы защиты ГИС [12]. Результатом решения этой задачи является уточненный набор мер защиты информации в ГИС. Эффективность защиты ГИС во многом определяется актуальностью угроз в банке угроз ФСТЭК России [19].

Поэтому необходимо оценить угрозы для информации в ГИС с устройствами терминального доступа.

В настоящий момент в банке угроз ФСТЭК России имеются описания следующих угроз, наиболее актуальных для терминальной архитектуры информационной системы:

- УБИ.006: Угроза внедрения кода или данных
- УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными
- УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети
- УБИ.084: Угроза несанкционированного доступа к

Таблица 2

Угрозы, специфичные для терминальной архитектуры ГИС

Table 2

Threats specific to the terminal architecture of state information systems

№ п/п	Наименование угрозы	Описание угрозы
1	Угроза аутентификации пользователя с чужого терминала	Угроза заключается в возможности авторизации пользователя с чужого терминала. При этом возможно нарушение требований защиты информации, доступной для этого пользователя вследствие отличающихся условий защиты информации на данном терминальном устройстве.
2	Угроза сохранения информации в долговременное хранилище терминала	Угроза заключается в сохранении информации на внешних накопителях терминального устройства без их последующей очистки.
3	Угроза невозможности сетевого подключения терминала (недоступность терминального сервера)	Угроза заключается в невозможности установления сетевого подключения терминального клиента к терминальному серверу.
4	Угроза чрезмерного использования вычислительных ресурсов терминального сервера в ходе интенсивного обмена межпроцессорными сообщениями	Угроза заключается в возможности возникновения ситуации типа «отказ в обслуживании» со стороны вычислительного поля терминального сервера.
5	Угроза трансляции в сессию накопителей информации со зловредным программным обеспечением	Угроза заключается в возможности внедрения вредоносного кода посредством трансляции в сессию накопителей информации.
6	Угроза неконтролируемого роста числа терминалов	Угроза заключается в возможности потребителями вычислительных мощностей терминального сервера подключения неограниченного числа терминальных устройств.
7	Угроза неопределённости ответственности за обеспечение безопасности терминальной архитектуры	Угроза заключается в возможности невыполнения ряда мер по защите информации как оператором терминального сервера, так и операторами терминальных устройств.

системе хранения данных из виртуальной и (или) физической сети

- УБИ.131: Угроза подмены субъекта сетевого доступа
- УБИ.170: Угроза неправомерного шифрования информации

Предлагается дополнить банк угроз ФСТЭК России угрозами, специфичными для терминальной архитектуры ГИС (таблица 2).

3. Результаты применения метода проблемного обучения в изучении дисциплины «Информационная безопасность»

Разработанная задача создания и разрешения проблемной ситуации по защите информации в ГИС с устройствами терминального доступа использована в изучении дисциплины «Информационная безопасность» в рамках проведения серии практических занятий. При этом такая организация позволила обеспечить целенаправленную учебно-познавательную деятельность студентов с поисковым характером в решении профессиональной задачи защиты информации в ГИС с устройствами терминального доступа.

В отличие от традиционных методов обучения, используемых на лекциях и семинарских занятиях, применение метода проблемного обучения способствует активизации индивидуальных и групповых исследований, приводит студентов к самостоятельным обобщениям, выводам и способствует выработке у студентов устойчивых практических навыков к самостоятельной работе [2].

При этом результативность процесса обучения следует оценивать, в первую очередь, по основным новообразованиям и трансформациям, которые формируются у студентов в их учебно-познавательной деятельности [21]. В частности, в данном случае в качестве показателя результативности студента, может быть, количество правильно обоснованных угроз информационной безопасности, отсутствующих в банке данных угроз ФСТЭК России.

Заключение

В данной работе рассмотрен метод проблемного обучения в предметной области «Информационная безопасность» на примере разработки задачи создания и разрешения проблемной ситуации по защите информации в ГИС с устройствами терминального доступа. Обоснована актуальность проблемы защиты информации в ГИС с устройствами терминального доступа [15]. Предложен способ разрешения проблемной ситуации на основе исследования модели тонких клиентов ГИС и взаимодействия сервера с тонкими клиентами, а также представлен результат исследования угроз информационной безопасности для модели тонких клиентов ГИС, отсутствующих в банке данных угроз ФСТЭК России и определены направления дальнейшего развития обеспечения информационной безопасности и защиты информации в ГИС с устройствами терминального доступа.

Применение метода проблемного обучения в изучении дисциплины «Информационная безопасность» с использованием разработанной задачи создания и разрешения проблемной ситуации по защите информации в ГИС с устройствами терминального доступа показало высокие результаты обучения студентов.

Литература

1. Шухов В.С., Володин Н.Н., Чучалин А.Г. Вопросы непрерывного медицинского образования (проблемно-ориентированное обучение) // Лечащий врач. 2000. № 3. С. 5–13.

2. Баклагова Ю.В. Проблемные методы обучения в образовательном процессе // Вопросы педагогики. 2019. № 11(1). С. 11–14.

3. Valentin S. Nikolaenko, Elena A. Grakhova, and Timur R. Rakhimov. Improving the Efficiency of the Educational Process Using Interactive Teaching Methods // SHS Web of Conferences 28(1):01073 С. 1–4.

4. Степанова О.М., Козлова Н.В., Крючков Ю.Ю., Соловьев М.А. Внедрение проблемно-ориентированных технологий в практику обучения студентов технических вузов // Известия Томского политехнического университета. 2006. Т. 309. № 1. С. 242–246.

5. Кухарев, Н. В. Эффективность обучения и воспитания. М.: Педагогика, 2014. 214 с.

6. Джуринский, А.Н. История педагогики и образования. XX-XXI века. М.: Юрайт, 2019. 282 с.

7. Бережнов С.В., Половко И.Ю. Применение бездисковых тонких клиентов в информационной системе персональных данных // Информационное противодействие угрозам терроризма. 2015. № 24. С. 306–308.

8. Кошкаров А.А. Структурная адаптация федеральных требований к медицинским информационным системам на региональном уровне // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2016. № 119. С. 889–925.

9. Губарева Т.В., Патрусова А.М. Центры обработки данных в Российской Федерации // Проблемы социально-экономического развития Сибири. 2015. № 2(20). С. 16–23.

10. Соловьев В.В. Улучшение защищенности распределенной информационной системы персональных данных на основе технологии

VPN и терминального доступа // Информационные технологии и проблемы математического моделирования сложных систем. 2017. № 18. С. 39–44.

11. Бочкарева Т.О. Обеспечение защиты информации ограниченного доступа, содержащейся в государственных информационных системах // III международный пенитенциарный форум «преступление, наказание, исправление» (к 20-летию вступления в силу Уголовно-исполнительного кодекса Российской Федерации). Сборник тезисов выступлений и докладов участников Международной научно-практической конференции. Академия ФСИН России. 2017. С. 363–366.

12. Татарникова Задача синтеза комплексной системы защиты информации в ГИС//Ученые записки РГГМУ. 2013. № 30. С. 204–211.

13. Сальников С.А., Цыбульский В.Г. Технология «тонкого клиента» и доверенная программная среда – ключевые направления повышения уровня информационной безопасности автоматизированных систем // Защита информации. Инсайд. 2008. № 2(20). С. 40–41.

14. Сизов В.А., Малиничев Д.М., Мочалов В.В. Совершенствование нормативно-правовой базы информационной безопасности для устройств терминального доступа государственной информационной системы // Открытое образование. 2020. № 24(2). С. 73–79.

15. Манышев В.В. Применение проблемного метода обучения в учебном процессе // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2006. № 1(7). С. 95–97.

16. Коротков С. Г., Крылов Д. А., Использование методов проблемного обучения при подготовке бакалавров профессионального обучения // Вестник Марийского государственного университета. 2017. № 1(25). Т. 11. С. 13–17.

17. Сальников С.А., Цыбульский В.Г., Технология «Тонкого клиента» и доверенная программная среда – ключевые направления повышения уровня информационной безопасности автоматизированных систем // Защита информации. Инсайд. 2008. № 2(20). С. 40–41.

18. Бражников А.Е. Роль стандартизации как категории организационно-правового обеспечения защиты информации в деятельности подразделений ФСТЭК России // Вестник Воронежского института МВД России. 2008. №1. С. 184–190.

19. Кошкаров А.А. Структурная адаптация федеральных требований к медицинским информационным системам на региональном уровне // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2016. № 119. С. 889–925.

20. Меры защиты информации в государственных информационных системах [Электрон. ресурс]. Методический документ ФСТЭК России от 11 февраля 2014 г. Доступ из справочно-правовой системы «КонсультантПлюс».

21. Болгарский А.И. Защита информации в государственных информационных системах // Вестник УрФУ. Безопасность в информационной сфере. 2011. № 2. С. 48–50.

References

1. Shukhov V.S., Volodin N.N., Chuchalin A.G. Issues of Continuing Medical Education (Problem-Oriented Learning). Lechashchiy vrach = Attending Physician. 2000; 3: 5–13. (In Russ.)

2. Baklagova YU.V. Problematic teaching methods in the educational process. Voprosy pedagogiki = Questions of pedagogy. 2019; 11(1): 11-14. (In Russ.)

3. Valentin S. Nikolaenko, Elena A. Grakhova, and Timur R. Rakhimov. Improving the Efficiency of the Educational Process Using Interactive Teaching Methods. SHS Web of Conferences 28(1):01073 S. 1-4.

4. Stepanova O.M., Kozlova N.V., Kryuchkov Yu.Yu., Solov'yev M.A. Implementation of problem-oriented technologies in the practice of teaching students of technical universities. Izvestiya Tomskogo politekhnicheskogo universiteta = Bulletin of the Tomsk Polytechnic University. 2006; 309; 1: 242-246. (In Russ.)

5. Kukharev, N. V. Effektivnost' obucheniya i vospitaniya = The effectiveness of training and education. Moscow: Pedagogika; 2014. 214 p. (In Russ.)

6. Dzhurinskiy, A.N. Istoriya pedagogiki i obrazovaniya. XX-XXI veka = History of pedagogy and education. XX-XXI centuries. Moscow: Yurayt; 2019. 282 p. (In Russ.)

7. Berezhnov S.V., Polovko I.Yu. The use of diskless thin clients in the personal data information system. Informatsionnoye protivodeystviye ugrozam terrorizma = Information countermeasures to terrorism threats. 2015; 24: 306-308. (In Russ.)

8. Koshkarov A.A. Structural adaptation of federal requirements for medical information systems at the regional level. Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta = Polythematic network electronic scientific journal of the Kuban State Agrarian University. 2016; 119: 889-925. (In Russ.)

9. Gubareva T.V., Patrusova A.M. Data processing centers in the Russian Federation. Problemy sotsial'no-ekonomicheskogo razvitiya Sibiri = Problems of social and economic development of Siberia. 2015; 2(20): 16-23. (In Russ.)

10. Solov'yev V.V. Improving the security of a distributed information system of personal data based on VPN technology and terminal

access. Informatsionnyye tekhnologii i problemy matematicheskogo modelirovaniya slozhnykh system = Information technologies and problems of mathematical modeling of complex systems. 2017; 18: 39-44. (In Russ.)

11. Bochkareva T.O. Ensuring the protection of restricted information contained in state information systems .III mezhdunarodnyy penitentsiarnyy forum «prestupleniye, nakazaniye, ispravleniye» (k 20-letiyu vstupleniya v silu Ugolovno-ispolnitel'nogo kodeksa Rossiyskoy Federatsii). Sbornik tezisov vystupleniy i dokladov uchastnikov Mezhdunarodnoy nauchno-prakticheskoy konferentsii. Akademiya FSIN Rossii = III International Penitentiary Forum "Crime, Punishment, Correction" (to the 20th anniversary of the entry into force of the Criminal Executive Code of the Russian Federation). Collection of abstracts of speeches and reports of the participants of the International Scientific and Practical Conference. Academy of the Federal Penitentiary Service of Russia. 2017: 363-366. (In Russ.)

12. Tatarnikova The task of synthesizing an integrated information security system in GIS. Uchenyye zapiski RGGMU = Uchenye zapiski RGGMU. 2013; 30: 204-211. (In Russ.)

13. Sal'nikov S.A., Tsybul'skiy V.G. Thin client technology and trusted software environment are the key directions for increasing the level of information security of automated systems. Zashchita informatsii. Insayd = Information Security. Inside. 2008; 2(20): 40-41. (In Russ.)

14. Sizov V.A., Malinichev D.M., Mochalov V.V. Improving the regulatory framework of information security for terminal access devices of the state information system. Otkrytoye obrazovaniye = Open Education. 2020; 24(2): 73-79. (In Russ.)

15. Manyshev V.V. Application of the problem teaching method in the educational process. Vestnik Belgorodskogo yuridicheskogo instituta MVD Rossii imeni I.D. Putilina = Bulletin of the Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilina. 2006; 1(7): 95-97. (In Russ.)

16. Korotkov S. G., Krylov D. A. The use of problem learning methods in the preparation of professional training bachelors. Vestnik Mariyskogo gosudarstvennogo universiteta = Bulletin of the Mari State University. 2017; 1(25); 11: 13-17. (In Russ.)

17. Sal'nikov S.A., Tsybul'skiy V.G. Thin Client Technology and Trusted Software Environment - Key Directions for Increasing the Information Security Level of Automated Systems. Zashchita informatsii. Insayd = Information Security. Inside. 2008; 2(20): 40-41. (In Russ.)

18. Brazhnikov A.Ye. The role of standardization as a category of organizational and legal support for information protection in the activities of subdivisions of the FSTEC of Russia. Vestnik Voronezhskogo instituta MVD Rossii = Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2008; 1: 184-190. (In Russ.)

19. Koshkarov A.A. Structural adaptation of federal requirements for medical information systems at the regional level. Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta = Polythematic network electronic scientific journal of the Kuban State Agrarian University. 2016; 119: 889-925. (In Russ.)

20. Measures of information protection in state information systems [Elektron. resurs]. Metodicheskiy dokument FSTEK Rossii ot 11 fevralya 2014 g. Dostup iz spravochno-pravovoy sistemy «Konsul'tantPlyus» = Methodological document of FSTEC of Russia dated February 11, 2014. Access from the reference legal system «ConsultantPlus». (In Russ.)

21. Bolgarskiy A.I. Information protection in state information systems. Vestnik UrFU. Bezopasnost' v informatsionnoy sfere = UrFU Bulletin. Information security. 2011; 2: 48-50. (In Russ.)

Сведения об авторах

Валерий Александрович Сизов
Д.т.н., профессор кафедры прикладной информатики и информационной безопасности Российский экономический университет им. Г.В. Плеханова», Москва, Россия
Эл. почта: Sizov.VA@rea.ru

Дмитрий Михайлович Малиничев
К.т.н., доцент кафедры информационных систем, сетей и безопасности Негосударственное образовательное частное учреждение высшего образования «Московский финансово-промышленный университет «Синергия», Москва, Россия
Эл. почта: mmm_63@list.ru

Information about the authors

Valery A. Sizov
Dr. Sci. (Engineering), Professor of the Department of Applied Informatics and Information Security Plekhanov Russian University of Economics, Moscow, Russia
E-mail: Sizov.VA@rea.ru

Dmitry M. Malinichev
Cand. Sci. (Engineering), Associate Professor of the Department of Information Systems, Networks and Security
Non-state educational private institution of higher education «Moscow Financial and Industrial University» Synergy», Moscow, Russia
E-mail: mmm_63@list.ru

Хамзат Хакимович Кучмезов
К.э.н., доцент,
Департамент «Бизнес-информатики»
Финансовый университет при Правительстве РФ, Москва, Россия
Эл. почта: kuchmezovx@gmail.com

Вадим Вячеславович Мочалов
Аспирант
Негосударственное образовательное частное учреждение высшего образования «Московский финансово-промышленный университет «Синергия», Москва, Россия
Эл. почта: vadimmoch@yandex.ru

Khamzat K. Kuchmezov
Cand. Sci. (Economics), Associate Professor
Department of Business Informatics
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: kuchmezovx@gmail.com

Vadim V. Mochalov
Postgraduate student
Non-state educational private institution of higher education «Moscow Financial and Industrial University» Synergy»,
Moscow, Russia
E-mail: vadimmoch@yandex.ru