УДК 74.48

КИБЕРУЧЕНИЯ И ИХ РОЛЬ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Н.А. Богульская (Красноярск, Россия)
М.М. Кучеров (Красноярск, Россия)
В.Б. Туговиков (Красноярск, Россия)

Аннотация

Проблема и цель. Практикоориентированность при подготовке специалистов по информационной безопасности нацелена на то, чтобы с первого дня работы на предприятии выпускники эффективно применяли полученные в вузе знания с учетом специфики той или иной отрасли. Это один из важных показателей качества образования. Необходимость повышения качества образования требует привлечения новых методов. *Целью* исследования является обоснование эффективности киберучений и киберполигонов для подготовки специалистов по информационной безопасности.

Методология исследования основана на сравнении новых подходов к обучению.

Результаты исследования. Выполнен анализ эффективности методов, применяемых для подготовки специалистов по информационной безопасности в Сибирском федеральном университете.

Заключение. Обоснована необходимость применения иммерсивных практико-ориентированных методов для подготовки специалистов по информационной безопасности.

Ключевые слова: *качество образования, информационная безопасность, киберучения, киберполигоны, профессиональные навыки, практикоориентированность, иммерсивность.*

Богульская Нина Александровна – кандидат физико-математических наук, доцент кафедры информационной безопасности, Сибирский федеральный университет (Красноярск); ORCID ID: 0000-0003-3144-0730; Scopus Author ID: 57194182313; e-mail: NBogulskaya@sfu-kras.ru

Кучеров Михаил Михайлович – кандидат физико-математических наук, доцент кафедры информационной безопасности, Сибирский федеральный университет (Красноярск); ORCID ID: 0000-0002-8432-5878; Scopus Author ID: 57193425132; e-mail: MKucherov@sfu-kras.ru

Туговиков Виктор Борисович – кандидат физико-математических наук, доцент кафедры информационной безопасности, Сибирский федеральный университет (Красноярск); e-mail: VTugovikov@sfu-kras.ru

Постановка проблемы. Кибербезопасность сегодня является необходимым условием успешной цифровой трансформации всех отраслей экономики [Доктрина ИБ, 2016; РФ. ФЗ № 149, 2006]. Практикоориентированность при подготовке специалистов по информационной безопасности (ИБ) нацелена на то, чтобы с первого дня работы на предприятии выпускники эффективно применяли полученные в вузе знания с учетом специфики той или иной отрасли. Знания передаются не только через лекции и учебники, но и путем проведения киберучений, через погружение студента в реальные кейсы и сценарии для отработки навыков противодействия киберугрозам.

Иммерсивные технологии обучения – это совокупность технических и педагогических методов и приемов, способствующих погружению и максимальному вовлечению обучающегося в искусственно созданную среду, в условия, приближенные к реальным. Иммерсивные технологии позволяют повысить эффективность образовательного процесса за счет передачи знаний студентам не только традиционным аудиовизуальным способом, но и в форме реального опыта и впечатлений, полученных в имитационной среде, построенной преподавателями исходя из реальных кейсов, связанных с выявлением и обработкой инцидентов ИБ в компаниях и организациях.

ВЕСТНИК КРАСНОЯРСКОГО ГОСУДАРСТВЕННОГО ПЕДАГОГИЧЕСКОГО УНИВЕРСИТЕТА им. В.П. АСТАФЬЕВА

Киберучения – отработка практических навыков реагирования на инциденты информационной безопасности специалистов по информационной безопасности, специалистов IT и пользователей информационных систем, подлежащих защите. Киберучения, не связанные с использованием средств вычислительной техники и сетевым оборудованием, ограниченные устным обсуждением и выработкой решений, называются **штабными киберучениями**.

Киберполигон – это комплекс программно-аппаратных решений, собранных в единую сеть для эмуляции действий реальной информационной инфраструктуры, по возможности полностью копирующий все протекающие в ней процессы, но не обрабатывающий какую-либо критичную информацию. Основное его назначение – отработка имитации кибератак, методов защиты и изучения инцидентов в условиях, максимально приближенных к реальным. Учебный киберполигон позволяет решить основную проблему – отсутствие реальной комплексной инфраструктуры для отработки навыков использования определенных средств и методов защиты данных и информационных ресурсов. Киберполигон позволяет проводить киберучения, которые делают аудиторные занятия более интересными и актуальными. Это дает реальный опыт защиты информационных систем, позволяет комплексно закрепить все полученные знания.

Проблема получения профессиональных навыков выпускниками Российских вузов обозначена уже как минимум с 2016 г.[1] Согласно исследованию Министерства науки и высшего образования, проведенному в 2020 г., 91 % работодателей признают недостаток практических навыков у выпускников вузов и более 40 % студентов считают, что обучение оторвано от требований рынка труда. Данная проблема касается и подготовки специалистов по направлению информационной безопасности.

Две основные причины отказа работодателями в трудоустройстве выпускников вузов – отсутствие опыта работы и плохая самопрезентация [Гурьянов, 2022]. Студентам направлений, связанных с информационной безопасностью, довольно сложно обеспечить качественные практические занятия, которые дадут навыки и знания для реальной работы по специальности, так как даже в ходе прохождения производственной и преддипломной практики организации, где уже выстроена система управления информационной безопасностью, не допускают обучающихся к реальным информационным процессам. Там, где требуется проведение исследований на предмет надежности системы ИБ, студентам не доверяют тестирование IT-инфраструктуры предприятия на наличие уязвимостей и даже не знакомят с системой управления ИБ. Эти ограничения оправданы, ведь даже раскрытие информации о применяемых методах и средствах защиты информации порой может нести угрозы информационной безопасности предприятия [Kucherov, Bogulskaya, 2017; 2018]. С другой стороны, на предприятия выпускники должны приходить с определенными практическими навыками. Данную коллизию можно разрешить при помощи проведения киберучений с использованием учебного киберполигона вуза.

Обзор научной литературы. Педагоги высшего образования отмечают необходимость повышения качества образования, подготовки специалистов с высоким уровнем готовности к профессиональной деятельности. Для технических вузов это вызвано динамизмом научно-технического прогресса.

Одним из ведущих направлений повышения качества образования называют формирование конкурентоспособности выпускников вузов [Ершова, Муллина, 2015]. При этом отмечается, что выпускники вузов часто проигрывают более опытным работникам из-за отсутствия профессиональных навыков [Гурьянов, 2023].

Необходимость повышения качества образования требует обновления форм, методов и средств обучения в вузах [Селеменева, 2016; Гринберг, 2011; Гринберг и др., 2017; Дрозд, 2023].

[1] Аналитический обзор ВЦИОМ. Контроль не ослаблять, качество повышать. 2016 г. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/vysshee-obrazovanie-kontrol-ne-oslablyat-kachestvo-povyshat

Киберучения – это один из новых форматов, учитывающий специфику подготовки специалистов по информационной безопасности [Анисимова, 2022]. Киберполигоны нужны не только для студентов, но и для уже действующих специалистов. При наличии учебного киберполигона сотрудники органов власти и предприятий могут повысить здесь свой уровень готовности к цифровым атакам, не нарушая реальные производственные процессы.

Результаты исследования. В статье выполнен анализ эффективности методов, применяемых для подготовки специалистов по информационной безопасности в Сибирском федеральном университете. Обоснован выбор формата киберучений.

В пользу киберучений говорят исследования, касающиеся эффективности учебного процесса. Эффективность подтверждается не только результирующим уровнем знаний и навыков студента, но и другими параметрами [Щеглова[2], 2021], а именно:

– успеваемость обучающегося, выраженная оценками в баллах;

– качество знаний, умений и навыков;

– уровень обучаемости, отражающий способность к усвоению знаний, и количество необходимой помощи для этого;

– степень адаптации выпускника вуза к жизни и профессиональной деятельности;

– темпы процесса самообразования;

– уровень общей образованности и приобретаемого профессионального мастерства;

– готовность к дальнейшему продолжению образования.

Эти показатели являются ключевыми для выбора студентом будущей деятельности, будь то поиск работы или продолжение образования.

В свете приобретения практических навыков у студентов специальностей, связанных с информационной безопасностью, рассматривают три метода ведения образовательной деятельности – пассивный, активный, интерактивный [Вербицкий, 1991; Захарова, 2008; Пак, Хегай, 2012; Роберт, 2010; Стебеняева, Ларина, 2016]. При этом интерактивный основан на продолжении и развитии идеи активного метода и становится еще более актуальным с применением иммерсивных технологий.

При пассивном методе, например на лекции, студенты получают знания от преподавателя в том виде, в котором его подготовил преподаватель, и не могут активно с ним взаимодействовать. Активный метод, применяемый, например, на семинаре, позволяет студентам влиять на ход проведения занятия, задавать вопросы, ставить проблемы или обсуждать материал с преподавателем во время занятия. Интерактивный метод является развитием активного и подразумевает взаимодействие студентов как с преподавателем, так и друг с другом, например в формате штабных киберучений. В ходе таких обсуждений обучающиеся либо действуют как одна команда экспертов, либо разделяются на несколько команд, и тогда занятие носит соревновательный характер [Хириев, 2007; Худякова, Давыдов, Васильев, 2011; Селезнева, Белая, Грузинцев, 2021].

Эффективное проведение киберучений требует от преподавателя умелого сочетания всех трех методов подачи материала [Осипов, 2022; Новиков, 2023; Olsson, Mozelius, Collin, 2015; Смирнов, 2010]. В ходе лекций или предварительной части семинарского занятия требуется наряду с теоретической частью, касающейся вопросов обеспечения информационной безопасности на предприятиях и в организациях, дать информацию о кейсах по реальным инцидентам информационной безопасности. Если в ходе киберучений предполагается использовать оборудование и программные средства учебного киберполигона, то предварительно необходимо дать описание возможностей данных конкретных технических решений. Это может быть описание DLP или SIEM-систем, межсетевых экранов, XDR-решений и т.д., которые будут применяться в киберучениях, проводимых с использованием учебного киберполигона. Желательно также дать описание

[2] Щеглова И.А. Взаимосвязь студенческой вовлеченности и образовательных результатов студентов российских университетов: дис. … канд. пед. наук. СПб., 2021. 112 с.

ВЕСТНИК КРАСНОЯРСКОГО ГОСУДАРСТВЕННОГО ПЕДАГОГИЧЕСКОГО УНИВЕРСИТЕТА им. В.П. АСТАФЬЕВА

встроенных средств контроля операционных систем, таких, например, как ведение и анализ электронных журналов событий, как одного из способов расследования инцидента ИБ.

Применение активного метода возможно на предварительной части подготовки к киберучениям в ходе семинарских занятий или в части лекционного занятия, где следует в ходе описания случаев из судебной практики, или из практики расследования инцидентов ИБ с применением средств защиты информации на предприятиях и в учреждениях вовлекать студентов в дискуссию о возможном ходе инцидента и его расследовании. Такое построение занятия позволит преподавателю при разработке сценария киберучений заранее распределить роли среди студентов.

Интерактивный метод применяется в ходе киберучений. Их проведение требует тщательного планирования занятия и следования определенному сценарию. Желательно при подготовке к занятию сформировать таблицы, где в первой колонке будет содержаться вопрос или описание этапа киберучений, количество остальных колонок определяется количеством команд, в них преподаватель проставляет оценки за каждый пройденный этап. Такие занятия позволяют обсуждать проблемы, максимально идентичные реальным кейсам из практики обеспечения информационной безопасности, а также призваны развивать у студентов навыки общения, работы в команде, формулирования итогов обсуждений и их грамотного описания. Независимо от того, выступают ли студенты как единая команда или две команды экспертов (это касается проведения штабных киберучений), делятся ли на «атакующих» и «защищающих» информационную систему, в командах необходимо назначить «капитана» и «технического писателя». При этом капитан команды должен координировать действия команды, отвечать за ведение дискуссии и принятие решений. Технический писатель при этом выполняет функцию регистрации хода киберучений, готовит письменный отчет о работе команды. Остальные члены команды помогают техническому писателю в формировании отчета.

Так как спецификой подготовки специалистов по информационной безопасности является отсутствие доступа к реальным средствам защиты на объектах информатизации, для формирования практических навыков работы необходимо использовать иммерсивные технологии. Навыки разборов ситуаций с нарушениями информационной безопасности, расследования инцидентов, отражения кибератак студенты приобретают в ходе киберучений и на учебных киберполигонах.

Киберучения безусловно являются самым эффективным подходом, повышающим качество образования по специальностям, связанным с информационной безопасностью. Как показала практика проведения практических занятий в виде киберучений, которые проводились преподавателями кафедры информационной безопасности института космических и информационных технологий Сибирского федерального университета для групп из 10 и более студентов, это помогает участникам в отработке навыков командной работы, коммуникативности, планирования и самоорганизации. Сама структура групповых киберучений подразумевает интенсивный обмен полученной информацией в процессе работы, развитие умения формулировать отчеты о ходе работ и мерах по расследованию инцидента.

Наличие учебного киберполигона крайне желательно для проведения практических занятий как со студентами, так и со слушателями курсов повышения квалификации и переподготовки. Есть мнение, что создание учебного кибер-полигона требует больших финансовых затрат и времени, а также обязательного привлечения внешних специалистов. Безусловно, на российском рынке есть компании, которые создают масштабные киберполигоны «под ключ», но стоимость таких решений оказывается неподъемной для бюджетов вузов. Вместе с тем для создания небольшой инфраструктуры, достаточной для обустройства учебного киберполигона, потребуются лишь одна или несколько компьютерных аудиторий и учебные лицензии программных средств обеспечения

информационной безопасности, которые могут быть предоставлены вендорами бесплатно или с большой скидкой, например в рамках договоров о сотрудничестве с вузом. При данном подходе может потребоваться лишь выделение средств на модернизацию серверов и компьютеров учебных аудиторий.

Ниже приведены примеры сценариев киберучений для студентов специальностей, связанных с информационной безопасностью.

Сценарий 1. Анализ подозрительного письма электронной почты.

Описание инцидента. Пользователь получил письмо, которое попало в папку SPAM, но так как в поле адреса отправителя была обозначена организация, с которой он ведет регулярную переписку, он открыл это письмо. Содержимое письма показалось ему странным, и он передал его специалистам по информационной безопасности.

Методические материалы. Архив, содержащий исходное письмо в формате HTML, скриншот экрана пользователя «New Fax Massage. pdf», RFC – заголовок письма в текстовом файле.

Задание. Требуется определить, является письмо СПАМом или фишингом, не несет ли оно какую-либо угрозу информационной безопасности, провести анализ и предложить меры, сделать общие выводы, сформулировать ответ пользователю и сообщение руководству организации.

Цели. Отработка навыков в распознавании фишинговой атаки, проведении анализа инцидента и его обработки.

Сценарий 2. Атака через фишинговое письмо.

Описание инцидента. Пользователь организации получил письмо со следующим содержанием: «Вам положены дополнительные выплаты, срок подачи документов истекает через сутки после отправки данного письма. Просим заполнить и направить нам по электронной почте заполненные и отсканированные бланки из прилагаемого архива». Письмо содержит вложение в виде самораспаковывающегося архива «Бланки документов». Пользователь запустил архив на самораспаковку, но не получил папку с документами, после повторного запуска на экране появился пляшущий человечек, после чего пользователь обратился в службу информационной безопасности.

Методические материалы. Виртуальная машина с ОС Winows, самораспаковывающийся архив WinRAR, выполняющий при автоматической распаковке следующий сценарий:

– инсталляция пакета r-admin;

– внесение изменений в реестр OCWindows;

– запуск анимации «Пляшущий человечек»;

– удаление следов инсталляции.

Задание. Требуется исследовать содержимое архива, переместив его на виртуальную машину, описать последовательность действий, которые выполняются на компьютере при запуске архива на автоматическую распаковку. Необходимо ответить на вопросы:

– какие цели мог преследовать создатель данного архива?

– какая угроза возникает после запуска архива на автоматическую распаковку?

– какие действия нужно выполнить для устранения угрозы, если пользователь запустил архив на разархивирование?

Необходимо сделать общие выводы по теме противодействия фишингу.

Цели. Отработка навыков анализа фишинговой атаки, применения виртуальной замкнутой среды для безопасного проведения анализа инцидента, его расследования.

Сценарий 3. Внутренняя угроза (нарушение целостности). Выполнение служебного расследования по факту подделки печати в договоре.

Описание инцидента. В ходе подготовки платежных документов в финансовом отделе организации выявлен договор, который не числится в основном реестре договоров организации. Оригинал документа не обнаружен, в ходе визуального анализа скан-копии договора установлено, что при помощи редактора изображений (вероятно, Photoshop) кем-то из пользователей в скан-копию не согласованного договора самовольно вставлена печать организации. Информация для расследования инцидента передана специалистам по информационной безопасности.

ВЕСТНИК КРАСНОЯРСКОГО ГОСУДАРСТВЕННОГО ПЕДАГОГИЧЕСКОГО УНИВЕРСИТЕТА им. В.П. АСТАФЬЕВА

Методические материалы. Виртуальная машина с предустановленными компонентами DLPSearchInform «Контур информационной безопасности», методические материалы.

Задание. Требуется определить, кто из инсайдеров внес несанкционированные изменения в договор, сделать общие выводы.

Цели. Отработка навыков проведения расследований при помощи компонентов DLP.

Заключение. Киберучения, в особенности проводимые с использованием учебного киберполигона, позволяют частично или полностью разрешить коллизию, связанную с отсутствием доступа обучающихся к реальным системам информационной безопасности, повысить их практические навыки. Применение иммерсивных практико-ориентированных методов для подготовки специалистов по информационной безопасности, к которым относятся киберучения, являются, по сути, единственным верным подходом в вопросах отработки практических навыков анализа ситуаций, связанных с инцидентами кибербезопасности. При этом необходимо учитывать все нюансы и аспекты, связанные как с внутренними, так и с внешними угрозами информационной безопасности. Обработка инцидентов, их анализ и выработка мер реагирования невозможны без применения специальных программно-аппаратных, других технических средств обеспечения информационной безопасности. В связи с этим необходимо сотрудничество вузов с производителями таких средств. Вендорам такое сотрудничество дает дополнительные возможности в продвижении своих продуктов, вузам – повышение качества подготовки специалистов через применение иммерсивных технологий обучения.

Библиографический список

1. Анисимова А. Защита от цифровых атак. Как в России работают киберполигоны // АНО «Национальные приоритеты». 2022. 21 июня. URL: https://национальныепроекты.рф/news/zashchita-ot-tsifrovykh-atak-kak-v-rossii-rabotayut-kiberpoligony
2. Вербицкий А.А. Активное обучение в высшей школе: контекстный подход. М.: Высшая школа, 1991. 207 с.
3. Гринберг Г.М. Инновационная модель выполнения выпускных квалификационных работ студентов на основе межвузовской кооперации // Инновации в непрерывном образовании. 2011. № 3. С. 14–19.
4. Гринберг Г.М., Дорошенко Е Г., Лукьяненко М.В., Пак Н.И., Савельева М.В. Профессиональная подготовка магистрантов в условиях инженерного образовательного кластера // Вестник КГПУ им. В.П. Астафьева. 2017. № 3 (41). С. 38–51. DOI: http://dx.doi.org/10.25146/1995-0861-2017-41-3-04
5. Гурьянов С. А вуз и ныне там: как выпускнику найти работу // Известия. 31 января – 13 апреля 2023 г. URL: https://iz.ru/1283700/sergei-gurianov/vuz-i-nyne-tam-kak-vypuskniku-naiti-rabotu
6. Доктрина информационной безопасности. Утверждена указом Президента РФ № 464 от 05.12.2016. URL: https://base.garant.ru/71556224
7. Дрозд А.В., Формы и форматы при обучении пользователей основам ИБ на примере темы паролей // SearchInform – Разработчик ПО для защиты информации / Статьи / Хабр/ 20 Июля 2023 г. URL: https://habr.com/ru/companies/searchinform/articles/749242
8. Ершова О.В., Муллина Э.Р. Формирование профессиональных компетенций студентов, обеспечивающих конкурентоспособность на рынке труда // Современные наукоемкие технологии. 2015. № 9. С. 133–136. URL: https://top-technologies.ru/ru/page/index
9. Захарова И.Г. Информационные технологии в образовании: учеб. пособие для студ. высш. учеб. заведений. М.: Академия, 2008. 192 с.
10. Новиков И. Обучение ИБ: как часто проводить и в каких формах. 2023. 10 марта. URL: https://www.anti-malware.ru/analytics/TechnologyAnalysis/Information-security-training

11. Осипов П. Есть такая профессия // Профсоюзная газета «Солидарность» Статьи. 2022. 30 ноября. URL: https://www.solidarnost.org/articles/est-takaya-professiya.html
12. Пак Н.И., Хегай Л.Б. Разработка трехмерных учебных материалов на основе гипертекстовой технологии // Инновации в непрерывном образовании. 2012. № 4. С. 78–84.
13. Роберт И.В. Современные информационные технологии в образовании: дидактические проблемы; перспективы использования. М.: ИИО РАО, 2010. 140 с.
14. Российская Федерация. Законы: Федеральный закон от 27.07.2006 № 149-ФЗ: редакция от 30 декабря 2021 года: с изменениями и дополнениями, вступившими в силу с 1 января 2022 // Консультант Плюс: справочная правовая система. URL: https://www.consultant.ru/document/cons_doc_LAW_61798
15. Селезнева Н.Т., Белая А.А., Грузинцев А.В. Психологические факторы использования личностью сетевых коммуникаций // Вестник КГПУ им. В.П. Астафьева. 2021. № 4 (58). С. 44–53.
16. Селеменева Т.А. Исследование эффективности образовательного процесса в условиях современного вуза // Проблемы и перспективы развития образования в России. Новосибирск: Центр развития научного сотрудничества, 2016. Вып. 43, т. 1. С. 98–102.
17. Стебеняева Т.В., Ларина Т.С. Об одном подходе к проектированию современных электронных образовательных ресурсов. Наука 21 века: вопросы, гипотезы, ответы. М.: Перо, 2016. № 1. С. 48–53.
18. Смирнов А.В. Образовательные кластеры и инновационное обучение в вузе: монография. Казань: РИЦ «Школа», 2010. 102 с.
19. Хириев А.Т. Теоретико-методологические основы информационной безопасности личности. 2007 (на правах рукописи). URL: https://www.daaudit.ru/news-pubs/pub-2-1.html
20. Худякова М.В., Давыдов С., Васильев В.Г. Классификация отзывов пользователей с использованием фрагментных правил. РОМИП, 2011.
21. Kucherov M.M., Bogulskaya N.A. Logical language of certificate-based access control in security models // ACM International Conference Proceeding Series. 2017. P. 131–135. DOI: 10.1145/3058060.3058067
22. Kucherov M.M., Bogulskaya N.A. Trilattice-based access control models // MatecWEB of Conferences. 2018. Vol. 210. 22nd International Conference on Circuits, Systems, Communications and Computers (CSCC 2018). DOI: 10.1051/matecconf/201821004053
23. Olsson M., Mozelius P., Collin J. Visualisation and gamification of e-Learning and programming education // Electronic Journal of E Learning. 2015. Vol. 13 (6). P. 441–454.

CYBER EXERCISES AND THEIR ROLE IN TRAINING INFORMATION SECURITY SPECIALISTS

N.A. Bogulskaya (Krasnoyarsk, Russia)
M.M. Kucherov (Krasnoyarsk, Russia)
V.B. Tugovikov (Krasnoyarsk, Russia)

Abstract

Statement of the problem. The practice-oriented approach to training information security specialists is aimed at ensuring that from the first day of work at an enterprise, graduates effectively apply the knowledge acquired at the university, taking into account the specifics of a particular industry. This is one of the important indicators of the quality of education. The need to improve the quality of education requires the use of new methods.

The purpose of the study is to substantiate the effectiveness of cyber exercises and cyber training grounds for training information security specialists.

The research methodology is based on the comparison of new approaches to teaching.

Research results. The article analyzes the effectiveness of methods used to train information security specialists at the Siberian Federal University.

Conclusion. The article substantiates the need to use immersive practice-oriented methods for training information security specialists.

Keywords: *quality of education, information security, cyber exercises, cyber training grounds, professional skills, practice-oriented, immersiveness.*

Bogulskaya, Nina A. – PhD (Physics and Mathematics), Associate Professor, Department of Information Security, Siberian Federal University (Krasnoyarsk, Russia); ORCID ID: 0000-0003-3144-0730; Scopus Author ID: 57194182313; e-mail: NBogulskaya@sfu-kras.ru

Kucherov, Mikhail M. – PhD (Physics and Mathematics), Associate Professor, Department of Information Security, Siberian Federal University (Krasnoyarsk, Russia); ORCID ID: 0000-0002-8432-5878; Scopus Author ID: 57193425132; e-mail: MKucherov@sfu-kras.ru

Tugovikov, Viktor B. – PhD (Physics and Mathematics), Associate Professor, Department of Information Security, Siberian Federal University (Krasnoyarsk, Russia); e-mail: VTugovikov@sfu-kras.ru

References

1. Anisimova A. Protection against digital attacks. How cyber ranges work in Russia // ANO “Natsionalnye prioritety” (ANO National Priorities), June 21, 2022. URL: https://nationalprojects.rf/news/zashchita-ot-tsifrovykh-atak-kak-v-rossii-rabotayut-kiberpoligony
2. Verbitsky A.A. Active learning in higher education: a contextual approach. Moscow: Vysshaya shkola, 1991. 207 p.
3. Grinberg G.M. Innovative model for completing final qualifying works of students based on interuniversity cooperation // Innovatsii v nepreryvnom obrazovanii (Innovations in Continuous Education). 2011. No. 3. P. 14–19.
4. Grinberg G.M., Doroshenko E.G., Lukyanenko M.V., Pak N.I., Savelyeva M.V. Professional training of undergraduates in the conditions of an engineering educational cluster // Vestnik KGPU im. V.P. Astafyeva (Bulletin of KSPU named after V.P. Astafyev). 2017. No. 3 (41). P. 38–51. DOI: http://dx.doi.org/10.25146/1995-0861-2017-41-3-04
5. Guryanov S. And the university is still there: how a graduate can find a job // Izvestia. January 31, 2022 – April 13, 2023. URL: https://iz.ru/1283700/sergei-gurianov/vuz-i-nyne-tam-kak-vypusknik-unaiti-rabotu
6. Information security doctrine, approved by Decree of the President of the Russian Federation No. 464 of December 5, 2016. URL: https://base.garant.ru/71556224

7. Drozd A.V. Forms and formats when teaching users the basics of information security using the example of passwords // SearchInform – Information security software developer / Articles / Habr / July 20, 2023. URL: https://habr.com/ru/companies/searchinform/articles/749242
8. Ershova O.V., Mullina E.R. Formation of professional competencies of students that ensure competitiveness in the labor market // Sovremennye naukoemkie tekhnologii (Modern Science-Intensive Technologies). 2015. No. 9. P. 133–136. URL: https://top-technologies.ru/ru/page/index
9. Zakharova I.G. Information technologies in education: manual for students of higher institutions. Moscow: Akademia, 2008. 192 p.
10. Novikov I. Information security training: how often to conduct and in what forms. March 10, 2023. URL: https://www.anti-malware.ru/analytics/ Technology Analysis/ Information-security-training
11. Osipov P. There is such a profession // Profsoyuznaya gazeta "Solidarnost" (Trade union newspaper "Solidarity"). November 30, 2022. URL: https://www.solidarnost.org/articles/est-takaya-professiya.html
12. Pak N.I., Khegai L.B. Development of three-dimensional educational materials based on hypertext technology // Innovatsii v nepreryvnom obrazovanii (Innovations in Continuous Education). 2012. No. 4. P. 78–84.
13. Robert I.V. Modern information technologies in education: didactic problems; prospects for use. Moscow: IIO RAO, 2010. 140 p.
14. Russian Federation. Laws: Federal Law No. 149-FZ dated July 27, 2006: as amended on December 30, 2021: with amendments and additions that came into effect on January 1, 2022 // Consultant Plus: reference legal system. URL: https://www.consultant.ru/document/cons_doc_LAW_61798
15. Selezneva N.T., Belaya A.A., Gruzintsev A.V. Psychological factors of a person's use of network communications // Vestnik KGPU im. V.P. Astafyeva (Bulletin of KSPU named after V.P. Astafyev). 2021. No. 4 (58). P. 44–53.
16. Selemeneva T.A. Study of the effectiveness of the educational process in the conditions of a modern university. In: Problems and Prospects for the Development of Education in Russia. Novosibirsk: OOO Tsentr razvitiya nauchnogo sotrudnichestva, 2016. Is. 43, vol. 1. P. 98–102.
17. Stebenyaeva T.V., Larina T.S. About one approach to the design of modern electronic educational resources // Nauka 21 veka: voprosy, gipotezy, otvety (Science of the 21st Century: Questions, Hypotheses, Answers). 2016. No. 1. P. 48–53.
18. Smirnov A.V. Educational clusters and innovative education in university: Monograph. Kazan: RITS "School", 2010. 102 p.
19. Khiriev A.T. Theoretical and methodological foundations of personal information security. 2007 (manuscript). URL: https://www.daaudit.ru/news-pubs/pub-2-1.html
20. Shcheglova I.A. The relationship between student engagement and educational results of Russian university students: PhD Thesis Summary (Education). St. Petersburg, 2021. 112 p.
21. Kucherov M.M., Bogulskaya N.A. Trilattice-based access control models // MatecWEB of Conferences. 2018. Vol. 210. 22nd International Conference on Circuits, Systems, Communications and Computers (CSCC 2018). DOI: 10.1051/matecconf/201821004053
22. Kucherov M.M., Bogulskaya N.A. Logical language of certificate-based access control in security models // ACM International Conference Proceeding Series. 2017. P. 131–135. DOI: 10.1145/3058060.3058067
23. Olsson M., Mozelius P., Collin J. Visualisation and gamification of e-Learning and programming education // Electronic Journal of E Learning. 2015. Vol. 13 (6). P. 441–454.

ВЕСТНИК КРАСНОЯРСКОГО ГОСУДАРСТВЕННОГО ПЕДАГОГИЧЕСКОГО УНИВЕРСИТЕТА им. В.П. АСТАФЬЕВА