

УДК 378.16

**РАЗРАБОТКА СИМУЛЯТОРА С ЭЛЕМЕНТАМИ ГЕЙМИФИКАЦИИ ДЛЯ
ПОВЫШЕНИЯ УРОВНЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ
БЕЗОПАСНОСТИ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА**

Смирнов Р. В.

(РГУ нефти и газа (НИУ) имени И. М. Губкина)

Научный руководитель – кандидат социологических наук, доцент Тагиров А. Р.

(РГУ нефти и газа (НИУ) имени И. М. Губкина)

Введение. В работе развивается тезис о качественном повышении уровня подготовки специалистов в области безопасности стратегически важного топливно-энергетического комплекса (ТЭК) и как следствие его защищенности при внедрении в образовательный процесс специальных компьютерных программ (симуляторов), позволяющих моделировать основные экономико-управленческие, технологические и информационные процессы предприятия и связанные с ними гибридные угрозы объекту ТЭК, а также симулировать и отрабатывать пользователям (специалистам в области безопасности и обучающимся разных образовательных программ) применение мер, направленных на нейтрализацию угроз и взаимодействие между собой для защиты условного объекта (согласно смоделированной ситуации).

Также автором предлагаются оптимальные параметры для формирования технического задания на разработку программы, предлагается подход к оценке экономического эффекта от эксплуатации программы в образовательных организациях и на предприятиях ТЭК, а также перспективы развития проекта.

Основная часть. Современный топливно-энергетический комплекс Российской Федерации является одним из факторов ее долгосрочного развития и стабильности: служит надежным поставщиком сырья и энергоресурсов для населения и предприятий, обеспечивает непрерывное функционирование и развитие ключевых отраслей экономики и науки, способствует развитию высокотехнологичной продукции. Указанные факторы формируют вклад отрасли в укрепление суверенитета и геополитического влияния России, что делает её стратегически важной и требует тщательного внимания к безопасности. Гибридный характер современных угроз безопасности формирует необходимость применения мер защиты в соответствии с теорией комплексной безопасности (ТКБ), которую определяют следующие направления: противодействие террористическим угрозам; противодействие киберугрозам; обеспечение правовой защиты предприятий; мобилизационная подготовка; антикоррупционная деятельность [1, с. 18]. Согласно ТКБ необходимо формировать принципиально иной подход к обеспечению безопасности – выстраивать многоуровневые системы безопасности с применением различных мер, способных как самостоятельно, так и в комплексе противостоять угрозам и самое главное - носить превентивный характер.

Одним из важнейших направлений управления персоналом на предприятии является работа по найму и обучению, однако зачастую выпускники, либо кандидаты на замещение должностей не имеют актуального опыта, а самое главное – практических навыков и компетенций, а также представления о характере деятельности и производственных процессах предприятия, что может негативно сказываться на качестве и своевременности выполнения работы, а также действий сотрудников при возникновении критических ситуаций, что особенно важно для специалистов по безопасности.

Одной из ключевых компетенций специалистов в области безопасности является способность представлять предприятие как совокупность взаимосвязанных экономико-управленческих, технологических и информационных процессов, что зачастую не всегда складывается у студентов – будущих сотрудников служб корпоративной защиты и руководителей. Также следует отметить необходимость понимания специалистами особенностей взаимодействия между коллегами других специализаций обеспечения

безопасности.

Наиболее эффективным способом отработки взаимодействия между подразделениями и специалистами при обеспечении безопасности объекта могут являться полноценные учения на объекте ТЭК с имитацией производственных процессов и актуальных угроз безопасности. Подобные мероприятия требуют значительных затрат, длительной подготовки и специализированных условий. Также в настоящее время разработаны и эксплуатируются платформы для закрепления узкоспециальных знаний. Например, кибер полигоны для специалистов по информационной безопасности – «Ampire» (компания «Перспективный мониторинг»), «Jet CyberCamp» («Джет Софт»), бизнес симуляторы – «Витрономика», а также различные обучающие системы справочных правовых систем «КонсультантПлюс» и «Гарант».

Автором предлагается разработать и внедрить в образовательный процесс подготовки компьютерные программы с применением инновационного метода геймификации, в которых моделируются основные процессы предприятия, представлены гибридные угрозы безопасности объектов ТЭК и существует возможность командного противостояния им. Геймификация – инновационный инструмент, подразумевающий внедрение элементов игры в неигровые процессы для повышения эффективности обучения (в образовании). Программа должна обеспечивать освоение и практическое применение знаний в области экономической, информационной и национальной безопасности; тренировку навыков и совершенствование компетенций, необходимых для выполнения ежедневных задач специалистов по обеспечению безопасности; получение пользователями междисциплинарных знаний о работе специалистов смежных профилей; обучение в условиях взаимодействия специалистов разных профилей между собой. Разработку предлагается разделить на модули: игровые механики, сценарии воздействия на объект, функционал пользователей (меры противодействия). Подобный подход позволит в дальнейшем также разрабатывать новые версии программы в соответствии с актуальными угрозами и мерами противодействия, а также применять программу при определенной доработке на предприятиях в других отраслях народного хозяйства

Подобный инструментарий в потенциале позволит качественно повысить уровень подготовки специалистов в области безопасности, что актуально в условиях существующего кадрового дефицита нефтегазовой отрасли и прогрессирующими гибридными воздействиями на объекты ТЭК и как следствие приведет к снижению убытков от инцидентов и получить экономический эффект от внедрения.

Выводы. Предложенный способ качественного повышения уровня подготовки специалистов в области комплексной безопасности ТЭК, основанный на внедрении компьютерных программ с элементами геймификации обладает новизной и может являться полезным. В дальнейшем планируется организация взаимодействия с образовательными организациями и хозяйствующими субъектами ТЭК для уточнения их требований к подобным решениям, формирование и уточнение аппарата оценки экономического эффекта от применения решения, а также формирование технического задания на разработку программы с учётом обратной связи, полученной от образовательных организаций и субъектов ТЭК.

Список использованных источников:

1. Правиков Д. И., Тагиров А. Р., Комплексная безопасность предприятий ТЭК: подходы к определению // Системы безопасности. 2023. №1. С. 16-19. URL: https://cs.groteck.ru/SS_1_2023/20/ (дата обращения 18.02.2025);
2. Лукьянчиков М. И., Лесных В. В., Инновационный подход к оценке экономической эффективности проактивных методов обеспечения комплексной безопасности // ТТПС. 2023. №2 (64). URL: <https://sciup.org/148326491> (дата обращения: 18.02.2025).