

*И. В. Лорич, И. М. Тюгаев*

## ПРИМЕНЕНИЕ ИГРОВЫХ ТЕХНОЛОГИЙ В ОБУЧЕНИИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Проанализированы основные игровые технологии, которые возможно применять в процессе обучения специалистов по информационной безопасности. Рассмотрены игровые процессы и инструменты, позволяющие обучающимся приобрести необходимые профессиональные навыки. Предложен комплексный курс игровых технологий, моделирующий деятельность специалистов по построению информационных систем, их защите и мониторингу безопасности.*

59

*The paper analyzes the basic gaming technologies that are possible for useful use in the process of education information security specialists. The game processes and tools that allow students to acquire the necessary professional skills are considered. A comprehensive course on the application of gaming technologies is proposed that simulates the activities of specialists of building information systems, protection and security monitoring.*

**Ключевые слова:** защита информации, информационная безопасность, игровые технологии в образовании.

**Keywords:** information protection, information security, gaming technology in education.

### Введение

Сегодня работодатели нуждаются в специалистах, способных исполнять свои должностные обязанности с использованием современных знаний и технологий здесь и сейчас, и специалисты по информационной безопасности — не исключение. Но мир информационных технологий постоянно меняется — как следствие, меняется и мир информационной безопасности, тесно связанный с ним. Возникает логичный вопрос: как научить человека тому, что будет актуально через несколько лет?

Один из ответов — использование игровых технологий. Используя игровые механики, можно не только научить человека добывать необходимую информацию для решения поставленной задачи, но и подогреть в нем игровой интерес для ее решения.

Почему люди играют в компьютерные игры? Игры — это интересно. Но это лишь вершина айсберга. Игры также — способ самореализации: они позволяют нам примерить роль, не свойственную в обычной жизни, добиться определенных успехов. Если говорить о мультиплеерных играх, то они дают возможность контактировать, коммуницировать и соревноваться с другими людьми.



## **Игровые технологии в образовании**

Игра — это вид деятельности, который выражается в способности человека преобразовывать действительность. Он нацелен на воссоздание и усвоение общественного опыта, где сформировывается и развивается самоуправление поведением [1]. Технология обучения — совокупность форм, методов, приемов и средств передачи социального опыта, а также техническое оснащение этого процесса [2]. Получается, игровая технология — это технология обучения, построенная на игровых принципах и специфических процессах — игровых механиках, позволяющих приобретать необходимые компетенции.

60

Проигрывая какой-либо процесс, мы получаем позитивный или негативный опыт. Позитивный опыт способствует приливу эндорфинов, мы чувствуем радость. Эндорфины же положительно воздействуют на процесс запоминания и «укладывают» информацию в долговременную память. А после получения негативного опыта в правильном учебном процессе должен идти анализ неверных действий, который в дальнейшем позволит получить опыт положительный.

Игровой сленг является частью игрового мира. В широком смысле под игровым сленгом понимают любые слова, используемые только в той или иной игре [3]. Его особенность в том, что у игроков отсутствует необходимость специального изучения слов. Значения слов игрового сленга «приклеиваются» к игроку в процессе раскрытия контекста игры. Тот же процесс возможно воспроизвести для изучения профессиональной терминологии, если применять ее в ходе игровой учебной деятельности.

### **Игровые процессы и инструменты в обучении специалистов по информационной безопасности**

Современные компьютерные игры наполнены большим количеством игровых процессов и инструментов, использование которых в совокупности позволяет разработчикам игр подогревать интерес к своим продуктам и не терять целевую аудиторию. Целевая аудитория учебных заведений — обучающиеся, от мотивации которых зачастую зависит приобретение «жестких» и «мягких» навыков.

Главным и основным игровым процессом, возможным для применения в образовании специалистов по информационной безопасности, является моделирование. Любая игра моделирует деятельность или даже целый набор деятельностей. Многим интересно почувствовать себя воином, полководцем-стратегом, гонщиком или даже летчиком-истребителем. Дидактические особенности этого процесса таковы, что в смоделированной деятельности игрок сначала выполняет ее интуитивно, а потом уже с опорой на свой опыт, увеличивая игровые показатели. Практически любой процесс из деятельности специалистов по защите информации возможно смоделировать — например, поиск уязвимостей или интеграцию средств защиты информации — не на пустых информационных ресурсах, а на приближенных к реальным.



Обучающийся не только привыкает к разнообразной инфраструктуре предприятия, но и учится правильно с ней взаимодействовать, чтобы не нанести вред.

Если смоделировать целую цепочку процессов, то мы получим другой широко распространенный игровой процесс — погружение. В игровых стратегиях и симуляторах погружение — неотъемлемая часть построения игры, заставляющая пользователя выполнять множество последовательно связанных действий, влияющих на общий исход игры. В информационной безопасности возможно погружать обучающихся в отдельные многопроцессные виды деятельности — такие, как построение комплексной защиты сетевой инфраструктуры целого предприятия или же этичный взлом-пентест. Обучающийся не только тренирует определенные профессиональные навыки, но и учится мыслить последовательно, заранее продумывая свои действия.

Многие виды игр построены на командном взаимодействии — игры-кооперативы. Их сюжет выстраивается таким образом, что задачи, которые ставятся перед геймерами, непосильны для решения одному человеку. В реальной деятельности успех выполнения проекта в установленные сроки зависит от набора знаний, навыков и действий сотрудников, выполняющих проект. Если моделирование строить для команды, то у обучающихся будут формироваться навыки командного взаимодействия — как социального, так и профессионального характера. При моделировании ситуаций из жизни специалистов по мониторингу безопасности, основанных на командном взаимодействии, у обучающихся будут развиваться навыки оперативных оценки ситуации и принятия решения.

Помимо самих игровых процессов, в играх есть и другие полезные материалы, применение которых возможно в образовательном процессе. Это игровые интерактивные инструменты: шкала успеха и система достижений и наград.

Организовав свой оценивающий сервис, в котором будут фиксироваться выполнение поставленных преподавателем задач и самые эффективные решения, мы получим систему по выявлению экспертов в определенных областях. Данные системы широко представлены в играх как элементы мотивации игроков. Интуитивно понятный интерфейс, доступность системы и приятный графический дизайн будут толчком для создания микросообщества экспертов, способных обмениваться опытом, полученным при выполнении игровых задач.

Шкалу успеха возможно использовать для графического представления обширных задач, поддержания интереса обучающегося на протяжении всего моделирования или погружения, а также представления освоенности курса в целом. Данный инструмент является частью всех сюжетных игр.

### **Комплексное применение игровых процессов**

Перечисленные в предыдущем разделе игровые процессы и инструменты применимы не только в высшем профессиональном образовании, но и в дополнительном.



Причем для дополнительного профессионального образования возможно использовать игровые технологии также на курсах повышения грамотности в сфере безопасности информации для сотрудников, не связанных непосредственно с защитой информации. Например, моделирование ситуации кражи данных — в чем люди ошибаются, на что обращать внимание.

Также отличным примером применения игровых технологий в дополнительном образовании будет повышение квалификации для специалистов информационной безопасности на основе моделирования эксплуатации новых уязвимостей и их устранения.

62

Принцип наставничества, при котором педагог лишь организует образовательный процесс, предоставляя подготовленные игровые площадки и необходимые базовые учебные материалы, активизирует процесс приобретения обучающимися «мягких» навыков, нацеленных на адаптацию своих действий, подбор необходимой информации и инструментария, а также «жестких» профессиональных навыков и опыта их применения в рабочем контексте.

Для высшего учебного заведения возможны внедрения как частичные, так и комплексные. Примером комплексного применения игровых технологий может стать курс, в котором обучающиеся делятся на группы — строителей, защитников и атакующих. Они сами строят информационную инфраструктуру различных типов организаций и предприятий, анализируют ее защищенность, создают систему защиты, мониторят ее безопасность, атакуют ее, предотвращают атаки и расследуют их. За это все обучающиеся получают достижения и награды, которые возможно отследить в специальной системе. Мы видим обучающий процесс в рамках одной большой игры с использованием специальных вычислительных и защитных средств, развернутых на платформе виртуализации. Дополнительную интерактивность курсу будет придавать шкала успеха прохождения. По итогам прохождения этапов курса следует анализ действий всех групп и ротация участников по видам деятельности. Результатом такого учебного процесса станет овладение большим количеством специальных и общих профессиональных навыков.

### **Заключение**

Частичное или комплексное использование игровых технологий в сочетании с выстроенным под них образовательным процессом может стать мощным механизмом обучения специалистов по информационной безопасности, способных ставить под сомнение аспекты организации любой деятельности с точки зрения ее безопасности.

Специалист сферы защиты информации должен понимать, как устроены программные продукты, как работают информационно-вычислительные сети и web-сервисы, какие существуют уязвимости в них и какие угрозы они в себе несут. При этом не забывая, что самым слабым звеном в любой цепи остаются люди.



### Список литературы

1. Алещугина Е. А., Ваганова О. И., Прохорова М. П. Методы и средства оценивания образовательных результатов студента вуза // Проблемы современного педагогического образования. 2018 № 59-3. С. 13-16
2. Воронин А. С., Словарь терминов по общей и социальной педагогике. Екатеринбург, 2006.
3. Сумцова О. В. Влияние английского языка на формирование компьютерного сленга в русском языке // Молодой ученый. 2011. №4. С. 241.

### Об авторах

Илья Валерьевич Лорич – ведущий специалист Центра мониторинга и защиты информационных систем ГАУ КО «Калининградский государственный научно-исследовательский центр информационной и технической безопасности»; ассист., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: lor4g@protonmail.com

Илья Михайлович Тюгаев – начальник Центра мониторинга и защиты информационных систем ГАУ КО «Калининградский государственный научно-исследовательский центр информационной и технической безопасности», Россия.

E-mail: tiugaev.i.m@gmail.com

### The authors

Ilya V. Lorch, Leading Specialist of the Center of Monitoring and Protection of Information Systems, Kaliningrad State Research Center of Information and Technical Security; Assistant, I. Kant Baltic Federal University, Russia.

E-mail: lor4g@protonmail.com

Ilya M. Tiugaev, Head of the Center of Monitoring and Protection of Information Systems, Kaliningrad State Research Center of Information and Technical Security, Russia.

E-mail: tiugaev.i.m@gmail.com