Введение

В современном мире информационная безопасность становится всё более актуальной проблемой. С ростом числа киберугроз и увеличением количества информации, которую мы передаём через интернет, возрастает необходимость в обучении студентов основам информационной безопасности. Одним из эффективных способов обучения является использование образовательных игр.

Актуальность темы

Образовательные игры становятся всё более популярными в образовательной среде. Они позволяют студентам учиться через игру, что делает процесс обучения увлекательным и запоминающимся. Кроме того, образовательные игры могут быть адаптированы под индивидуальные потребности каждого студента, что позволяет обеспечить более эффективное обучение.

Однако, несмотря на все преимущества образовательных игр, их использование в обучении информационной безопасности всё ещё недостаточно распространено. Это связано с тем, что многие преподаватели не знакомы с преимуществами этого подхода и не знают, как его правильно применять. Также существует недостаток исследований, которые бы подтверждали эффективность образовательных игр в обучении информационной безопасности.

Таким образом, актуальность данной работы заключается в необходимости изучения и анализа использования образовательных игр в процессе обучения информационной безопасности. Необходимо определить, какие именно образовательные игры наиболее эффективны, как они влияют на успеваемость студентов и какие проблемы могут возникнуть при их использовании.

Цель и задачи проекта

Целью данного проекта является разработка и внедрение образовательной игры по информационной безопасности для студентов первого курса. Для достижения этой цели необходимо решить следующие задачи:

1. Изучить теоретические основы использования образовательных игр в обучении.

2. Проанализировать опыт применения образовательных игр в различных учебных заведениях.

3. Определить критерии эффективности образовательных игр по информационной безопасности.

4. Разработать образовательную игру по информационной безопасности, которая будет соответствовать критериям эффективности.

5. Провести эксперимент по применению образовательной игры в одном из учебных заведений.

6. Оценить результаты эксперимента и сделать выводы о влиянии образовательной игры на успеваемость и мотивацию студентов.

7. Подготовить отчёт о результатах исследования и разработать методические рекомендации для преподавателей по использованию образовательных игр в обучении информационной безопасности.

8. Рассмотреть перспективы дальнейшего развития образовательных игр и их использования в обучении информационной безопасности.

Решение этих задач позволит получить более полное представление об использовании образовательных игр в обучении информационной безопасности и разработать рекомендации, которые помогут преподавателям эффективно использовать этот подход в своей работе.

Определение проблемы

В современном мире информационная безопасность становится всё более актуальной проблемой. С ростом числа киберугроз и увеличением количества информации, которую мы передаём через интернет, возрастает необходимость в обучении студентов основам информационной безопасности. Однако, несмотря на все преимущества образовательных игр, их использование в обучении информационной безопасности всё ещё недостаточно распространено. Это связано с тем, что многие преподаватели не знакомы с преимуществами этого подхода и не знают, как его правильно применять. Также существует недостаток исследований, которые бы подтверждали эффективность образовательных игр в обучении информационной безопасности.

Таким образом, проблема заключается в том, что образовательные игры по информационной безопасности не получили широкого распространения в образовательной среде. Необходимо определить, какие именно образовательные игры наиболее эффективны, как они влияют на успеваемость студентов и какие проблемы могут возникнуть при их использовании.

Для решения этой проблемы необходимо провести исследование, которое позволит определить критерии эффективности образовательных игр по информационной безопасности и разработать образовательную игру, соответствующую этим критериям.

Альтернативные подходы

1. **Использование традиционных методов обучения:** лекций, семинаров, практических занятий и лабораторных работ. Это позволит студентам получить базовые знания и навыки в области информационной безопасности.

2. **Внедрение новых технологий в процесс обучения:** использование онлайн-курсов, видеолекций, интерактивных заданий и симуляторов. Это сделает обучение более интересным и доступным для студентов.

3. **Организация стажировок и практик в компаниях, занимающихся информационной безопасностью.** Это позволит студентам применить полученные знания на практике и получить опыт работы в этой области.

4. **Создание специализированных курсов по отдельным темам информационной безопасности:** криптографии, защите от киберугроз, управлению доступом и т. д. Это поможет студентам углубить свои знания в конкретных областях.

5. **Проведение мастер-классов и семинаров с участием экспертов в области информационной безопасности.** Это даст студентам возможность получить ценные знания и советы от профессионалов.

6. **Разработка и внедрение системы оценки знаний и навыков студентов в области информационной безопасности.** Это позволит отслеживать прогресс каждого студента и корректировать программу обучения в соответствии с его потребностями.

7. **Сотрудничество с компаниями, занимающимися информационной безопасностью, для организации совместных проектов и исследований.** Это будет способствовать развитию практических навыков студентов и их профессиональному росту.

8. **Развитие системы наставничества и менторства для студентов.** Это поможет им получить поддержку и помощь от опытных специалистов в области информационной безопасности.

Анализ конкурентов:

Анализ конкурентов							
Критерий оценки		**Книги**	**Лекции**	**Электронные книги / Форумы**	**Курсы**	**Проект "ZeroSpace"**	**CTF**
1	**Стоимость**	Малая/средняя стоимость. (средняя от 300р. до 1200р.)	Входят в стоимость обучения. Зачастую имеются открытые записи лекций в бесплатном доступе.	Большая часть материала находится в открытом доступе бесплатно.	Крайне высокая стоимость. (средняя от 2000р.)	Бесплатный.	Бесплатный. (Есть исключения)
2	**Удобство**	Не электронный формат. Книги занимают место. Некоторые книги могут быть слишком тяжелыми и большими для свободного ношения с собой.	Требуют посещения занятий и личного присутствия. Большая часть лекций не записывается и требует конспектирования.	Электронный формат. Читаются в любое свободное время пользователя.	Электронный формат.	Электронный формат. Можно играть в любое свободное время. Игра подразумевает в себе наличие развлекательных элементов, делающих процесс обучения проще.	Электронный формат. Требует высокой мыслительной нагрузки и сосредоточенности на задаче.
3	**Теоретические знания**	Высокие теоретические знания.	Высокие теоретические знания. Зачастую включают в себе ценный опыт самих выступающих, который сложно найти в интернете или печатном материале.	Высокие теоретические знания. Разные форумы могут в общей совокупности раскрыть темы более подробно чем книги.	Высокие теоретические знания.	Высокие теоретические знания. Каждая методика взлома подробно объясняется, а также раскрываются второстепенные темы, не менее важные для студента по ИБ.	Большая часть CTF подразумевает уже наличие каких-либо знаний студента. Очень малая часть CTF объясняют методы взлома. Требуются сторонние ресурсы для прохождения непонятных этапов.
4	**Практические знания**	Практика отсутствует.	Практика отсутствует.	Практика отсутствует.	Подразумевает практическую работу с пользователем, но не гарантирует её и не отслеживает правильность выполнения работы.	Высокие практические знания. ZeroSpace подробно описывает каждую методику взлома для игрока, объясняя все необходимые шаги для успешного решения искусственно поставленной проблемы.	Высокие практические знания.

Календарный план:

Название проекта: ZeroSpace

Руководитель проекта: Паюсов К.Д.

Таблица 1 – Календарный план

№	Название	Ответственный	Длительность	Дата начала	Временные рамки проекта			
					1 нед	2 нед	3 нед	4 нед
Анализ								
1.1	*Определение проблемы*	Руководитель проекта	1 неделя	Начало проекта	x	-	-	-
1.2	*Выявление целевой аудитории*	Руководитель проекта, аналитик	2 недели	Начало проекта	x	x	-	-
1.3	*Конкретизация проблемы*	Руководитель проекта	3 дня	Начало проекта	x	-	-	-

1.4	*Подходы к решению проблемы*	Руководитель проекта	5 дней	| Начало проекта	x	-	-	-
1.5	*Анализ аналогов*	Аналитик	7 дней	Начало проекта	x	-	-	-
1.6	*Определение платформы и стека для продукта*	Разработчик	4 дня	Начало проекта	x	-	-	-
1.7	*Формулирование требований к MVP продукта*	Руководитель проекта, разработчик	1 неделя	Начало проекта	x	-	-	-
1.8	*Определение платформы и стека для MVP*	Разработчик	2 дня	Начало проекта	x	-	-	-
1.9	*Формулировка цели*	Руководитель проекта	2 дня	Начало проекта	x	-	-	-
1.10	*Формулирование требований к продукту*	Руководитель проекта, аналитик	1 неделя	Начало проекта	x	-	-	-
1.11	*Определение задач*	Руководитель проекта	3 дня	Начало проекта	x	-	-	-
Проектирование								
2.1	*Архитектура системы (компоненты, модули системы)*	Разработчик	1 неделя	После определения требований	x	-	-	-
2.2	*Разработка сценариев использования системы*	Разработчик	3-4 дня	После разработки архитектуры	-	x	-	-

2.3	*Прототипы интерфейсов*	Дизайнер	3-4 дня	После разработки сценариев	-	x	-	-
2.4	*Дизайн-макеты*	Дизайнер	1 неделя	После прототипов	-	x	x	-
2.5	*Архитектура системы (компоненты, модули системы)*	Разработчик	3 недели	После определения требований	x	-	-	-
Разработка								
3.1	*Написание кода*	Разработчик	4 недели	После утверждения дизайна	x	x	x	x
3.2	*Тестирование приложения*		4 недели	Параллельно с написанием кода	x	x	x	x
Внедрение								
4.1	*Оформление MVP*	Руководитель проекта, дизайнер	2 дня	После завершения тестирования	-	-	-	x
4.2	*Внедрение MVP*	Руководитель проекта	7 дней	После оформления MVP	-	-	-	x
4.3	*Написание отчета*	Аналитик	2 недели	Параллельно с внедрением	-	-	x	x
4.4	*Оформление презентации*	Дизайнер	5 дней	Перед защитой проекта	-	-	-	x

	Защита проекта	Вся команда	1 день	07.06 - 15.06	-	-	-	x

Сценарии использования образовательной игры по информационной безопасности

1. Знакомство с основами информационной безопасности.

Цель: познакомить студентов с основными понятиями и принципами информационной безопасности.

Сценарий: игра начинается с вводного урока, на котором студенты знакомятся с понятием информационной безопасности, её целями и задачами. Затем они проходят серию заданий, которые помогают им понять, как работает информационная безопасность и какие меры необходимо предпринимать для её обеспечения.

2. Изучение методов защиты от киберугроз.

***Цель*:** научить студентов методам защиты от различных видов киберугроз.

Сценарий: в игре представлены различные виды киберугроз, такие как фишинг, вирусы, DDoS-атаки и т. д. Студенты должны научиться распознавать эти угрозы и принимать меры по их предотвращению. Для этого они могут использовать различные инструменты и методы защиты, такие как антивирусное ПО, фаерволы, шифрование данных и т. п.

3. Практические задания по защите информации.

Цель: дать студентам возможность применить полученные знания на практике.

Сценарий: после изучения теории студенты переходят к практическим заданиям, в которых они должны защитить информацию от различных киберугроз. Задания могут быть разнообразными, например, настроить фаервол, зашифровать данные, обнаружить и устранить вирус и т. д.

4. Тестирование системы на уязвимости.

Цель: обучить студентов тестированию систем на уязвимости.

Сценарий: студенты изучают методы тестирования систем на уязвимости, такие как сканирование портов, анализ трафика, поиск уязвимостей в коде и т. п. Затем они применяют эти методы к виртуальной системе, чтобы найти и исправить уязвимости. Это позволяет им лучше понять, как работают хакеры и как им противостоять.

5. Анализ инцидентов информационной безопасности.

Цель: научить студентов анализировать инциденты информационной безопасности и принимать соответствующие меры.

Сценарий: студентам предоставляется описание инцидента информационной безопасности, такого как утечка данных, взлом системы или DDoS-атака. Они должны проанализировать инцидент, определить его причины и последствия, а также предложить меры по предотвращению подобных инцидентов в будущем.

6. Решение задач по информационной безопасности.

Цель: проверить знания и навыки студентов в области информационной безопасности.

***Сценарий*:** студентам предлагается решить ряд задач по информационной безопасности, таких как выбор правильного пароля, настройка фаервола.

Требования к продукту и MVP

1. Требования клиентов:

- Продукт должен быть интересным и увлекательным для студентов первого курса направления «Информационная безопасность».

- Игра должна способствовать усвоению основных понятий и принципов информационной безопасности.

- В игре должны быть представлены различные виды киберугроз, чтобы студенты могли научиться распознавать их и принимать меры по их предотвращению.

- Задания должны быть разнообразными и интересными, чтобы поддерживать мотивацию студентов.

- Система тестирования на уязвимости должна быть реалистичной и приближённой к реальным условиям.

- Анализ инцидентов информационной безопасности должен быть основан на реальных событиях.

2. Функциональные требования:

- Наличие вводного урока, на котором студенты знакомятся с понятием информационной безопасности, её целями и задачами.

- Возможность прохождения серии заданий, которые помогают студентам понять, как работает информационная безопасность и какие меры необходимо предпринимать для её обеспечения.

- Представление различных видов киберугроз в игре.

- Предоставление инструментов и методов защиты от киберугроз.

- Проведение практических заданий по защите информации.

- Тестирование системы на уязвимости.

- Анализ инцидентов информационной безопасности.

- Решение задач по информационной безопасности.

3. Нефункциональные требования:

- Простота использования.

- Доступность для всех студентов первого курса.

- Безопасность данных.

- Надёжность работы.

- Адаптивность под разные устройства.

- Поддержка разных языков.

- Совместимость с другими образовательными платформами.

4. Производные требования:

- Разработка руководства пользователя.

- Создание обучающих видеоуроков.

- Обеспечение технической поддержки.

- Регулярное обновление контента.

- Мониторинг отзывов пользователей.

- Внесение изменений на основе обратной связи.

Стек для разработки образовательной игры по информационной безопасности на Unreal Engine

1. **Unreal Engine 5** — игровой движок, который предоставляет инструменты для создания игр различных жанров. Он имеет множество функций и возможностей, которые могут быть полезны при разработке образовательной игры.

2. **Blueprints** — визуальный язык программирования, который позволяет создавать игровые механики без написания кода. Это может быть полезно для начинающих разработчиков, а также для тех, кто хочет быстро создать прототип игры.

3. **C++** — язык программирования, который используется для более сложных задач, таких как оптимизация производительности, работа с данными и т. д.

4. **Visual Studio Code** — интегрированная среда разработки, которая может использоваться для написания кода на C++. Она имеет множество расширений и плагинов, которые могут упростить процесс разработки.

5. **Git** — система контроля версий, которая позволяет отслеживать изменения в коде и возвращаться к предыдущим версиям. Это важно для обеспечения качества кода и совместной работы над проектом.

6. **GitHub** — веб-сервис для хостинга проектов с открытым исходным кодом. Может быть использован для хранения кода, документации и других файлов проекта.

7. **UE Marketplace** — магазин плагинов и ресурсов для Unreal Engine. Здесь можно найти множество инструментов и материалов, которые могут помочь в разработке игры.

8. **Unreal Marketplace** — официальный магазин контента для Unreal Engine, где можно приобрести готовые ассеты, модели, звуки и другие ресурсы для использования в своих проектах.

9. **Substance Painter** — программа для создания текстур и материалов для 3D-моделей. Может использоваться для создания реалистичных поверхностей и эффектов.

10. **Adobe Photoshop** — растровый графический редактор, который может использоваться для редактирования изображений и создания новых.

Прототипирование

1. **Определение целей и задач прототипа.** На этом этапе мы должны определить, какие функции образовательной игры по информационной безопасности мы хотим проверить с помощью прототипа. Например, мы можем создать прототип, который будет проверять работу системы тестирования на уязвимости или анализ инцидентов информационной безопасности.

2. **Создание макета.** Макет — это упрощённое представление продукта, которое позволяет нам быстро и дёшево проверить его основные функции. Мы можем создать макет в виде блок-схемы, диаграммы или даже просто описать его словами.

3. **Тестирование прототипа с пользователями**. После создания макета мы должны протестировать его с реальными пользователями, чтобы получить обратную связь о его удобстве использования,

функциональности и других характеристиках. Это поможет нам выявить проблемы и внести необходимые изменения в продукт.

4. **Доработка прототипа на основе обратной связи.** После тестирования мы должны проанализировать полученную обратную связь и определить, какие изменения необходимо внести в прототип. Мы также можем провести дополнительные тесты, чтобы убедиться, что внесённые изменения улучшили продукт.

5. **Повторное тестирование прототипа.** После внесения изменений мы должны повторно протестировать прототип, чтобы убедиться, что он соответствует нашим требованиям. Если прототип не соответствует требованиям, мы должны вернуться к шагу 3 и повторить процесс.

6. **Завершение прототипа**. Когда прототип соответствует нашим требованиям, мы можем завершить его разработку и перейти к следующему этапу проекта.

Проектирование и разработка образовательной игры по информационной безопасности

1. **Анализ требований к продукту.** На этом этапе мы должны проанализировать требования, которые были определены на предыдущих этапах проекта. Мы должны убедиться, что продукт соответствует потребностям целевой аудитории и решает поставленные задачи.

2. **Выбор платформы и стека для разработки.** Мы должны выбрать платформу, на которой будет разрабатываться игра, и стек технологий, который будет использоваться для её создания. Мы можем использовать различные платформы, такие как Unreal Engine, Unity или Godot, а также различные языки программирования, такие как C++, Python или JavaScript.

3. **Разработка архитектуры системы.** Архитектура системы определяет структуру и взаимодействие компонентов системы. Мы должны разработать архитектуру, которая будет соответствовать

требованиям к продукту и обеспечивать его надёжность, масштабируемость и удобство использования.

4. **Создание сценариев использования.** Сценарии использования определяют, как пользователи будут взаимодействовать с системой. Мы должны создать сценарии, которые будут соответствовать целям и задачам продукта.

5. **Дизайн-макеты.** Дизайн-макеты — это визуальное представление интерфейса системы. Мы должны создать дизайн-макеты, которые будут привлекательными, понятными и удобными для пользователей.

6. **Написание кода**. Написание кода — это процесс создания программного обеспечения, которое реализует функциональность системы. Мы должны написать код, который соответствует архитектуре системы и обеспечивает её работоспособность.

7. **Тестирование приложения.** Тестирование — это процесс проверки работоспособности и качества программного обеспечения. Мы должны провести тестирование приложения, чтобы убедиться, что оно работает правильно и не содержит ошибок.

8. **Внедрение MVP**. MVP (Minimum Viable Product) — это первая версия продукта, которая имеет только основные функции. Мы должны внедрить MVP, чтобы получить обратную связь от пользователей и определить, какие функции необходимо добавить в следующие версии продукта.

9. **Оформление MVP.** Оформление MVP — это создание документации, инструкций и других материалов, которые помогут пользователям понять, как использовать продукт. Мы должны оформить MVP, чтобы обеспечить его доступность и понятность для пользователей.

10. **Внедрение.** Внедрение — это процесс распространения продукта среди пользователей. Мы должны внедрить продукт, чтобы он стал доступен для целевой аудитории.

11. **Тестирование и доработка.** После внедрения мы должны провести тестирование продукта на реальных пользователях, чтобы выявить проблемы и внести необходимые изменения. Мы также можем провести дополнительные тесты, чтобы улучшить качество продукта.

12. **Завершение разработки.** Когда продукт соответствует требованиям, мы можем завершить разработку.

Заключение

В ходе выполнения проекта была разработана образовательная игра по информационной безопасности для студентов первого курса. Игра представляет собой интерактивный обучающий инструмент, который позволяет студентам изучать основы информационной безопасности в увлекательной и доступной форме.

Игра включает в себя следующие основные компоненты:

* вводный урок, на котором студенты знакомятся с понятием информационной безопасности, её целями и задачами;

* серию заданий, которые помогают студентам понять, как работает информационная безопасность и какие меры необходимо предпринимать для её обеспечения;

* представление различных видов киберугроз в игре;

* предоставление инструментов и методов защиты от киберугроз;

* проведение практических заданий по защите информации;

* тестирование системы на уязвимости;

* анализ инцидентов информационной безопасности;

* решение задач по информационной безопасности.

Для разработки игры использовался игровой движок Unreal Engine 5. В процессе разработки были использованы следующие инструменты и технологии:

* Blueprints — визуальный язык программирования;

* C++ — язык программирования для более сложных задач;

* Visual Studio Code — интегрированная среда разработки;

* Git — система контроля версий;

* GitHub — веб-сервис для хостинга проектов с открытым исходным кодом;

* UE Marketplace — магазин плагинов и ресурсов для Unreal Engine;

* Unreal Marketplace — официальный магазин контента для Unreal Engine.

Прототипирование включало в себя создание макета игры и его тестирование с пользователями. Результаты тестирования показали, что игра является интересной и полезной для студентов. Она помогает им лучше усвоить материал и повысить мотивацию к изучению информационной безопасности.

Перспективы дальнейшей разработки темы включают в себя расширение функционала игры, добавление новых уровней сложности и возможностей для взаимодействия с другими игроками. Также возможно создание дополнительных образовательных игр по другим темам информационной безопасности.