Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина» (УрФУ)

Институт радиоэлектроники и информационных технологий – РТФ

ОТЧЕТ
О проектной работе
по теме: 1C25S. Образовательная игра
по дисциплине: Проектный практикум 1А

Команда: Фантом.std

Тимлид: Воскресенский Олег РИ-140943

Программист: Бочкарёв Павел РИ-140943

Аналитик: Сидорова Дарья РИ-140943

Дизайнер: Черных Мирослава РИ-140941

Геймдизайнер: Тулянкин Владимир РИ-141004

Екатеринбург

2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном мире, пронизанном цифровыми технологиями, вопросы кибербезопасности приобретают первостепенное значение. Стремительное развитие информационных технологий и повсеместное проникновение интернета в нашу жизнь привели к появлению новых угроз и рисков, связанных с информационной безопасностью. Особенно уязвимы перед киберпреступниками дети и подростки, активно пользующиеся онлайн-сервисами и социальными сетями, зачастую не обладающие достаточными знаниями и навыками для защиты от киберугроз.

Существующие образовательные программы по кибербезопасности, как правило, ориентированы на специалистов и профессионалов в сфере IT, в то время как необходимо формировать культуру кибербезопасности среди широких слоев населения, начиная со школьного возраста. Традиционные методы обучения, такие как лекции и семинары, часто оказываются недостаточно эффективными для привлечения внимания и удержания интереса молодежи к сложной теме кибербезопасности. Наблюдается явный дефицит интерактивных и увлекательных образовательных материалов, способных в доступной форме познакомить детей и подростков с основными принципами защиты информации и научить их распознавать и противостоять киберугрозам. Таким образом, существует противоречие между необходимостью формирования культуры кибербезопасности у молодежи и недостаточным количеством эффективных и привлекательных образовательных инструментов.

В связи с этим, разработка и внедрение образовательных игр по кибербезопасности представляется актуальной и перспективной задачей, способной существенно повысить уровень осведомленности и готовности молодежи к противостоянию киберугрозам.

Цель проекта: Разработка образовательной игры, направленной на повышение уровня осведомленности и формирование навыков в области кибербезопасности у подрастающего поколения.

Задачи проекта:

1. Изучить существующие образовательные игры по кибербезопасности и выявить их сильные и слабые стороны;
2. Определить целевую аудиторию и ее возрастные особенности для разработки соответствующего игрового контента;
3. Разработать концепцию и сценарий образовательной игры, включающие интерактивные задания, головоломки и моделирование реальных ситуаций, связанных с киберугрозами;
4. Реализовать разработанную концепцию в виде интерактивной компьютерной игры на кроссплатформенной среде разработки компьютерных игр Unity;
5. Провести испытание разработанной игры на целевой аудитории и оценить ее эффективность в формировании знаний и навыков в области кибербезопасности.

1. Целевая аудитория

Для успешной реализации поставленных задач и достижения цели проекта необходимо четко определить целевую аудиторию образовательной игры. С этой целью будет использована методика 5W Марка Шеррингтона[1], которая позволит провести детальный анализ потенциальных пользователей и учесть их потребности и интересы при разработке игрового контента.

1. Кто? (Who?)

Молодежь, с 16 до 24 лет, заинтересованная в повышении своей цифровой грамотности и расширении знаний в области кибербезопасности. Также их объединяет стремление быть защищенными в цифровом мире и интерес к интерактивному обучению.

2. Что? (What?)

Образовательная игра, направленная на:

- Ознакомление с основными концепциями и терминами в области кибербезопасности.
- Демонстрацию практического применения теоретических знаний.
- Развитие навыков решения проблем и принятия решений в ситуациях, связанных с киберугрозами.
- Игра может включать элементы симулятора, стратегии и головоломки, а также интерактивные тесты и викторины.

3. Почему? (Why?)

Потребность/мотивация:

- Повысить свою осведомленность в вопросах кибербезопасности;
- Получить базовые знания и навыки в области кибербезопасности;
- Подготовиться к будущей профессии, связанной с информационными технологиями;
- Интересно и увлекательно провести время, играя и обучаясь одновременно;

- Удовлетворить любопытство и интерес к взлому и защите информации (безопасным способом!).

Проблемы, которые решает игра:

- Недостаток знаний и навыков в области кибербезопасности у молодежи;
- Нехватка интересных и увлекательных образовательных материалов по данной теме;
- Необходимость привлечь внимание к важности кибербезопасности среди молодежи.

4. Когда? (When?)

Потребность в образовательной игре по кибербезопасности возникает в следующих ситуациях: выбор будущей профессии, поиск интересного способа углубления знаний в IT, желание разобраться в проблемах кибербезопасности после новостей о кибератаках.

5. Где? (Where?)

Дома (компьютер), в библиотеке, на онлайн-платформах образовательных учреждений, на образовательных сайтах.

2. Определение проблемы

Современная молодежь, вступающая во взрослую жизнь, является активным пользователем интернета и цифровых технологий [2]. Она проводит значительную часть времени в социальных сетях, общается в мессенджерах, играет в онлайн-игры, совершает покупки в интернете и использует онлайн-сервисы для учебы и развлечений. Эта активная онлайн-жизнь делает её особенно уязвимой для различных киберугроз.

Несмотря на цифровой бум, уровень цифровой грамотности и знаний в области кибербезопасности у многих молодых людей остается недостаточным. Это приводит к ряду проблем [3]:

1. Неосознанное раскрытие личной информации (Молодежь часто бездумно делится личной информацией в социальных сетях, не осознавая потенциальных последствий);
2. Слабые пароли и их повторное использование (Многие используют простые и легко угадываемые пароли, а также повторяют их для разных учетных записей, что делает их уязвимыми для взлома);
3. Нераспознавание фишинговых атак (Недостаток опыта и критического мышления делает молодежь легкой добычей для фишинговых атак, цель которых – кража логинов, паролей и банковских данных);
4. Загрузка вредоносного программного обеспечения (Неосторожная загрузка файлов и посещение подозрительных сайтов может привести к заражению устройств вредоносным программным обеспечением);
5. Кибербуллинг и онлайн-преследование (Молодые люди часто становятся жертвами и участниками кибербуллинга, что может иметь серьезные психологические последствия);
6. Непонимание конфиденциальности данных (Незнание правил и настроек конфиденциальности в социальных сетях и других

онлайн-сервисах приводит к неконтролируемому распространению личной информации);

7. Недостаток критического мышления при потреблении онлайн-контента (Вера в фейковые новости и дезинформацию может приводить к принятию неверных решений и формированию искаженного представления о реальности).

Традиционные методы обучения кибербезопасности, такие как лекции и учебники, часто кажутся молодежи скучными и неинтересными. Необходим более увлекательный и интерактивный подход, который позволит молодым людям в игровой форме освоить ключевые концепции кибербезопасности и развить практические навыки защиты в цифровом мире.

3. Подходы к решению проблемы

Мы предлагаем разработать образовательную онлайн-игру под названием «Un1t», ориентированную на обучение навыкам защиты от киберугроз и мошеннических схем для молодого поколения. Название Un1t выбрано, чтобы отразить дух интернет-сленга и сделать его запоминающимся. Игра позволит игрокам почувствовать себя ценной единицей команды, чтобы научиться автоматизировать свою работу, а затем использовать эти знания для эффективной работы.

Ключевым элементом образовательной игры «Un1t» является набор ключевых особенностей, каждая из которых тщательно продумана для обеспечения максимальной вовлеченности и эффективности обучения:

1. Режим игры: Игрок будет решать определенные задачи, имитирующие действия хакеров. Цель – понять, как работает взлом изнутри. Важно подчеркнуть, что игра рассчитывает на получение знаний о том, как хакеры получают наши данные тем или иным способом, поэтому все действия происходят в безопасной, контролируемой среде и не направлены на нанесение реального ущерба;
2. Процесс обучение: Перед каждым уровнем игроку будет даваться небольшая теория (ознакомление с методом взлома) и после у него будет возможности проверить полученные знание в виде теста. За каждый правильный ответ будет поощрение в виде дополнительных апгрейдов или навыков, которыми он сможет воспользоваться при прохождении уровня;
3. Реалистичный сценарий: Игра будет моделировать реальные киберугрозы, с которыми подростки могут столкнуться в повседневной жизни. Каждый уровень по-своему уникален и направлен на определенный метод взлома [4] («Брутфорс», «Фишинг», «Троян», «Сниффер»), а значит игрок по итогу

прохождения игры будет знать несколько способов, как люди «попадают в лапы» мошенников.

Все эти элементы создадут захватывающий и познавательный опыт, направленный на формирование у игроков прочных навыков в области кибербезопасности.

Игра «Un1t» преследует четко определенные учебные цели, направленные на формирование у игроков не только теоретических знаний, но и практических навыков, необходимых для успешной защиты от киберугроз, а именно:

- Понимание принципов работы хакеров и их методов;
- Освоение навыков защиты от киберугроз и мошеннических схем;
- Развитие критического мышления и умения анализировать информацию;
- Повышение осведомленности о кибербезопасности и формирование ответственного поведения в интернете.

Таким образом, «Un1t» разработан специально для молодежи, которых объединяет желание повысить свою цифровую грамотность, углубить знания в кибербезопасности, защитить себя в цифровом мире и получить эти знания в интерактивной, захватывающей форме. Игра предоставит им уникальную возможность взглянуть на мир глазами хакера, тем самым вооружив необходимыми знаниями и навыками для эффективной защиты от киберугроз.

4. Анализ аналогов

Для того, чтобы правильно определить наших аналогов нужно тщательно проанализировать как прямых, предлагающих образовательные игры по кибербезопасности, так и косвенных, предоставляющих альтернативные способы получения знаний в этой области, например, онлайн-курсы и учебные пособия.

Для оценки конкурентной среды в сфере обучения кибербезопасности для молодежи был проведен анализ как игровых продуктов, так и образовательных курсов. При этом особое внимание уделялось платформам, предлагающим именно игровой формат обучения (Hackmud [5], TryHackMe [6], Uplink [7]). Среди косвенных аналогов были рассмотрены популярные онлайн-курсы: "Специалист по кибербезопасности" от Skillbox и "Специалист по кибербезопасности-"Белый хакер" от Skillfactory.

Определим, что именно будем сравнивать у аналогов. Составим таблицу, в которой будут подробно описаны следующие пункты:

1. Небольшое описание курса/игры
2. Обучение
3. Стоимость и время обучения
4. Адаптация под уровень пользователя

Для вывода сделаем небольшую таблицу, в которой выделим основные сильные и слабые стороны курса/игры (Таблица 1):

Таблица 1 - Сравнение аналогов

Аналоги	Сильные стороны	Слабые стороны	Выводы
Skillbox "Специалист по кибербезопасности"	**Комплексное обучение**: Полный спектр тем, начиная с защиты серверов и заканчивая законодательством в сфере кибербезопасности. **Поддержка экспертов**: Опытные	**Финансовые затраты**: Обучение требует значительных финансовых вложений. **Временные обязательства**: Программа подразумевает	Отлично подходит для новичков, желающих получить структурированные знания и официальное подтверждение квалификации. Однако, будьте

	преподаватели и менторы готовы помочь в освоении материала. **Сертификация**: Подтверждает навыки и повышает шансы на трудоустройство.	длительное обучение. **Теоретический перевес**: Практические навыки могут уступать объему теоретического материала.	готовы к значительным инвестициям времени и денег.
«Белый» хакер. Специалист по кибербезопасности от Skillfactory	**Практическая направленность**: Упор на пентест и этичный хакинг, востребованные в современной кибербезопасности. **Узкая специализация**: Глубокое погружение в конкретную область кибербезопасности.	**Стоимость курса**: Как и любое качественное обучение, требует финансовых вложений. **Ограничение кругозора**: Подходит только тем, кто уже определился со специализацией в пентесте.	Прекрасный выбор для тех, кто уже имеет базовые знания и хочет стать профессионалом в области пентеста и этичного хакинга. Если интересует более широкий спектр тем, стоит рассмотреть другие варианты.
Hackmud	**Уникальный геймплей**: Обучение происходит в увлекательной игровой форме в стиле киберпанк. **Доступная цена**: Низкая стоимость по сравнению с другими курсами и платформами.	**Ограниченный функционал**: Не охватывает все аспекты кибербезопасности. **Устаревшая графика**: Визуальное оформление может не понравиться современным пользователям.	Отличный вариант для тех, кто хочет освоить азы хакинга в игровой форме и не готов тратить много денег. Важно учитывать, что это не полноценный курс, а скорее развлечение с элементами обучения.
TryHackMe	**Практический опыт**: Обучение основано на отработке навыков взлома и защиты систем на виртуальных машинах. **Гибкость и доступность**: Можно выбирать модули и	**Технические требования**: Для комфортной работы требуется стабильное интернет-соединен ие и достаточно мощный компьютер. **Языковой барьер**: Большая часть	Идеально подходит для тех, кто предпочитает практический опыт, готов самостоятельно изучать материалы на английском языке и имеет необходимые

	темы, учиться в удобном темпе. Есть бесплатный контент для ознакомления.	контента на английском языке.	технические ресурсы.
Uplink	**Ролевой элемент:** игроки берут на себя роль хакера и выполняют разнообразные задания. **Образовательный эффект:** изучение основ кибербезопасности и взлома. **Разнообразие заданий:** задания разной сложности и нелинейный сюжет поддерживают интерес.	**Отсутствие адаптивного обучения:** новичкам может быть сложно освоиться. **Цена:** относительно высокая стоимость игры. **Время прохождения:** может сильно варьироваться в зависимости от стиля игры.	Игра подходит любителям хакерских симуляций и тем, кто хочет изучить основы кибербезопасности. Разнообразие заданий и сюжет делают её интересной, но отсутствие адаптивного обучения, цена и сложность могут затруднить начало для новичков.

Анализ конкурентов показал, что на рынке не хватает образовательной игры по кибербезопасности, которая сочетала бы в себе достаточный охват тем, оптимальную цену и необходимый уровень адаптации, ориентированный на начинающих пользователей. Разрабатываемая игра будет позиционироваться как интерактивный способ познакомиться с основами кибербезопасности, с акцентом на практические навыки и интерактивное обучение. Игра позволит погрузиться в мир кибербезопасности в развлекательной форме и получить базовые знания о ключевых угрозах и способах защиты.

5. Дизайн-документ

5.1. Вводные данные

Платформа – ПК

Игровой движок – Unity

Язык – русский

Жанр – 2D игра с видом сверху, с элементами жанра roguelike

5.2. Игровые локации

Каждый игровой уровень представляет собой комнаты, соединенные переходами. В каждой комнате игрок сражается с волнами врагов, но в конце каждого уровня игровой процесс будет отличаться. Каждый уровень открывается после успешного прохождения предыдущего (Рисунок 1):

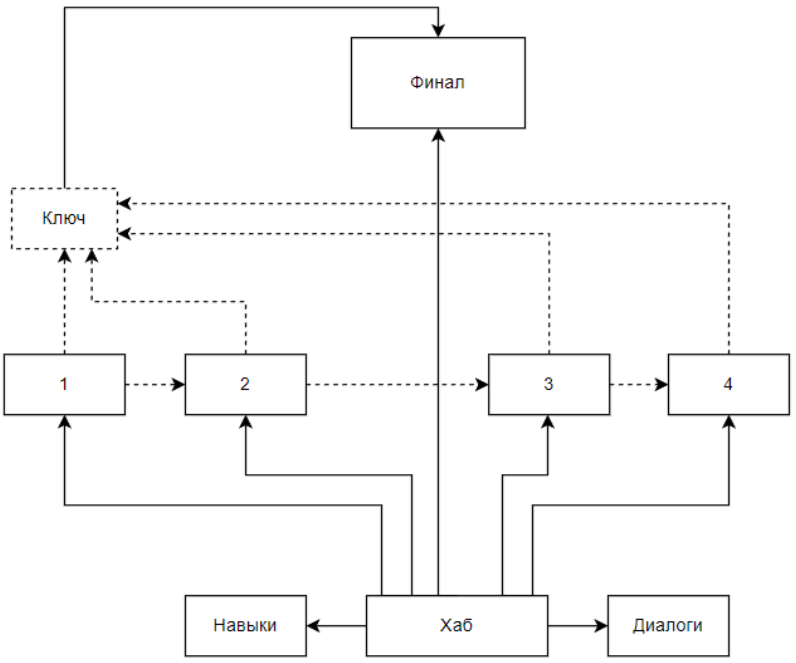


Рисунок 1 - Схема игровой карты

5.3. Главный экран

Главный экран стилизован под рабочий стол компьютера. Основные элементы интерфейса:

- Выбор уровней – ярлыки приложений на главном экране;

- Выбор навыков – папка с ярлыками, обозначающие навыки, при наведении мышкой на ярлык всплывает описание;
- Перепросмотр диалогов обучения – папка “Logs” с “текстовыми документами”, запускающими диалог.

5.4. Уровни

5.4.1. Уровень “Брутфорс”

Данный уровень самый простой – в финальной комнате игроку необходимо выжить, сражаясь против волн появляющихся врагов, определенное количество времени, пока идет процесс “подбора пароля”.

5.4.2. Уровень “Сниффер”

Финальная комната представляет собой лабиринт, игроку предстоит собрать кусочки “трафика”, раскиданные по нему, чтобы открыть выход.

В данном лабиринте появляются усиленные (почти бессмертные) враги, строго следующие определенному пути передвижения. Игроку нужно будет запомнить передвижения врагов в этом лабиринте, чтобы пройти незамеченным. В случае, если игрока заметили, все враги на уровне направляются в его сторону. Игрок может попробовать пройти к выходу, несмотря на преследующих и атакующих врагов, или вернуться ко входу в лабиринт и дождаться, когда враги о нем забудут.

5.4.3. Уровень “Троян”

На данном уровне финальная комната отсутствует. Для прохождения игроку необходимо будет пройти комнаты, собрать достаточное количество “очков информации” чтобы заполнить шкалу “информации”, и после этого выйти из уровня через стартовую комнату. Однако параллельно со временем заполняется шкала “уровня подозрительности” – если она достигнет максимума раньше, чем шкала информации, уровень будет провален. Таким образом, она работает как скрытый таймер, ограничивающий время на прохождение.

5.4.4. Уровень ”Фишинг”

В финальной комнате игроку необходимо будет убедить игрового персонажа открыть доступ к следующему уровню системы. Игрок должен будет выбрать правильные варианты диалога за короткий промежуток времени – аналог системы “Quick Time Event”.

5.4.5. Финал игры

Данный уровень не будет иметь комнат в обычном понимании – игрок сразу появляется в финальной комнате перед процессором, который ему необходимо атаковать. Однако довольно быстро становится понятно, что атаки игрока никак не влияют на процессор, поэтому для прохождения игроку необходимо будет сначала атаковать менее защищенные системы,. Игрока будет перемещать в несколько подуровней, которые являются укороченными вариациями прошедших уровней. Таким образом игроку дается возможность закрепить материал. По прохождению всех подуровней, игрок “захватывает” системы менее защищенных пользователей, таким образом “клонируется” и проводит успешную атаку на процессор.

5.5. Игровой процесс

5.5.1. Основные механики

5.5.1.1. Управление:

Передвижение производится с помощью нажатия на клавиши “W”, “A”, “S”, “D”.

Дальняя атака производится путем зажатия левой кнопки мыши, ближняя – с помощью нажатия на правую кнопку мыши.

Рывок производится на пробел, следует курсору

Направление атаки следует курсору.

Использования одного из 3 типов спец. навыков производится на кнопки “1”, “2” и “3”.

5.5.1.2. Атака:

Существует 2 типа атаки – дальняя и ближняя.

Дальняя атака представляет собой выпускание снарядов в направлении курсора, наносит урон врагам, столкнувшимся со снарядом. Снаряды выпускаются с определенным интервалом, пока зажата правая кнопка мыши.

Ближняя атака представляет собой нанесение урона врагам в области перед игроком. Атака производится путем одиночного нажатия на левую кнопку мыши, есть определенный кулдаун.

5.5.2. Комнаты

Каждый уровень (кроме Финала) представляет собой от 8 до 12 комнат, соединенных коридорами, а также стартовую комнату и финальную (если она есть).

Все комнаты представляют собой прямоугольники одного размера, их размещение на уровне случайно, коридоры всегда соединяют центры сторон комнат. Комнаты выбираются случайным образом из списка заранее заготовленных комнат, в них отличается размещение точек появления врагов, препятствия.

При входе в комнату с врагами выходы блокируются. Комната считается пройденной, когда игрок побеждает все волны врагов, после этого проходы разблокируются.

5.5.3. Система вознаграждений

После прохождения комнаты с определенным шансом в ней может появиться сундук, до 5 раз за уровень. Для его открытия игроку необходимо правильно ответить на вопрос с двумя вариантами ответа по теме, рассматриваемой на текущем уровне (подробнее Процесс обучения, пункт 2).

После успешного открытия сундука из него выпадает один случайный пассивный апгрейд (см. Приложение А).

С побежденных врагов с определенным шансом выпадает некоторое количество “очков информации” – валюты, с помощью которой можно покупать навыки на стартовом экране. Шанс выпадения и количество зависит от типа врага и сложности на уровне.

5.5.4. Враги

5.5.4.1. Генерация волн врагов

В каждой комнате есть 5-8 точек появления врагов. Одна волна врагов – некоторое количество одновременно появившиеся из данных точек врагов, после победы над ними появляется следующая волна (см. Приложение Б).

На уровне есть невидимая шкала “сложности”, она зависит от времени нахождения на уровне. С помощью нее производятся:

- расчет количества волн;
- расчет шанса появления врага;
- расчет шанса появления врага более сложного класса.

5.5.4.2. Типы врагов

В зависимости от сложности врага меняется их дизайн, размер, кол-во здоровья, паттерн поведения и атака. В каждом классе сложности есть подклассы “Ближняя атака” и “Дальняя атака”.

Легкие:

- Тип “Ближняя атака” – атакуют игрока только когда он столкнулся с ним;
- Тип “Дальняя атака” – раз в определенное время выпускают снаряд по направлению в игрока;

Сложные

- Тип “Ближняя атака” – атакуют игрока когда он находится рядом с ним: если игрок попадает в первичную зону поражения, враг останавливается, “замахивается” (показывается основная зона поражения врага), и производит атаку по основной зоне, если игрок не ушел из первичной;
- Тип “Дальняя атака” – раз в определенное время выпускают несколько снарядов по направлению в игрока.

5.5.5. Апгрейды

5.5.5.1. Пассивные (получают в игровом процессе):

- Скорость передвижения (Увеличивает скорость передвижения);
- Скорость атаки (Увеличивает скорость атаки);
- Скорость регенерации здоровья (Увеличивает скорость регенерации здоровья);
- Урон ближней атаки (Увеличивает урон от дальних атак);
- Урон дальней атаки (Увеличивает урон от ближних атак).

5.5.5.2. Навыки (покупают на стартовом экране)

В игре будут называться “эксплойтами”.

Данные навыки игрок может активировать с определенным кулдауном (раз в несколько секунд) при нажатии на клавишу на клавиатуре

Игрок одновременно может выбрать только 3 активных навыка, изменить свой выбор он может только в стартовой локации (см. Приложение В).

- "Логическая бомба" – через определенное время после активации наносит урон врагам вокруг игрока;
- "Червь" – игрок может заразить врага, заставляя его атаковать ближайших союзников;
- “Перегруз” – игрок может на несколько секунд обездвижить всех врагов в комнате;
- “Бэкап” – игрок один раз за уровень может оставить свою “копию”, после смерти игрок перемещается в место, где он её оставил;
- “Спуфинг” – игрок может на несколько секунд замаскироваться под программу, тем самым исчезая для врагов. Покупка данного навыка открывается после прохождения уровня “Троян”;
- "Переадресация" – на несколько секунд активируется щит, урон от атак врагов отправляется ближайшим врагам. Открывается после прохождения уровня “Фишинг”.

5.5.6. Процесс обучения

Элементы обучения глубоко интегрированы в повествовательную часть игры – сюжет. В начале каждого уровня игроку в виде диалога дается информация о том, как хакеры используют рассматриваемый на этом уровне метод взлома, а также как это предотвращают специалисты по информационной безопасности. Также небольшие комментарии даются героями в процессе сражения и после прохождения комнат.

При открытии сундука у игрока начинается выбор ответа из 2 вариантов.

При выборе неправильного ответа, меню выбора закрывается, начинается диалог с Главной по ИБ, где она рассказывает про рассматриваемый вопрос, после чего игрок может еще раз попытаться открыть сундук.

При выборе правильного ответа с первой попытки, обучающий диалог также начинается но с измененным текстом.

В случае неправильного ответа автоматически запускается диалог с персонажем Адой (Главной по Информационной Безопасности): она подробно объясняет суть вопроса, а затем игрок получает возможность вновь попытаться открыть сундук.

В случае правильного ответа с первой попытки также запускается обучающий диалог, однако его текст отличается – в нём Ада хвалит игрока и дает дополнительные разъяснения.

В конце уровня, перед его завершением, у игрока начинается мини-викторина. Случайным образом выбирается 3 вопроса из тех, что были заданы при открытии сундуков на данном уровне, если игрок правильно ответил на все – он может закончить уровень. В ином случае ему придется переиграть данный уровень (см. Приложение Г).

Некоторая информация дается в виде текста в описании апгрейдов.

5.5.7. Пример диалога (Акт 3, перед уровнем “Троян”)

(см. Приложение Д)

Ада:

Цикада, слушай внимательно. Операция классифицируется как скрытое внедрение по методу "троянского коня". Ты будешь замаскирован под стандартный процесс системы путем изменения твоей "цифровой подписи", антивирус посчитает тебя обычной программой, если действовать быстро. Задача – собрать данные об ИИ, копируя фрагменты его кода.

Цикада:

О, типа того как вирусы прячутся в пиратских играх? Круто! А если я замешкаюсь?

Ада:

Каждый системный процесс имеет свой шаблон поведения. Антивирус мониторит аномалии в программах, они не должны потреблять ресурсы сверх нормы долгое время. Если это произойдет – начнется сканирование. В лучшем случае – процесс будет прерван. В худшем – С.П.А.М. поймет, что это не глюк, а вторжение.

Цикада:

Понял-понял! Кстати, а почему именно троян? Разве нельзя было просто...

Ада:

58% всех вредоносных атак – это трояны. Они эффективны и опасны тем, что пользуются доверием. Пользователи часто даже не замечают подмены, сами скачивают и запускают, а антивирусы пропускают их из-за поддельных сертификатов. Спиратенная программа, драйвера для принтера, даже обычный pdf-файл с электронной почты - все что угодно может содержать вирус. (Вздыхает.) Мы сами блокировали подобные атаки, а теперь используем такие методы.

Цикада:

Ага, вместо паролей мы крадём... э-э, "заимствуем" код!

Ада:

Если бы существовал стандартный протокол для таких ситуаций!.. я бы!.. (Пауза.) Просто помни: один неверный шаг – и «маскировка» рухнет.

Цикада:

Не волнуйся! Я же сам как троян – с сюрпризом!

Ада:

...Просто вернись с данными. И целым…

5.5.8. Пример вопроса для “сундука” и обучающего диалога

Что важно для троянской программы, чтобы она сработала?

Правильный ответ:

Доверие пользователя

Диалог:

Ада:

Верно, Цикада. Троян полагается на обман. Пользователь должен поверить, что программа полезна или безобидна, и сам запустить её. Как мы замаскировались под системный процесс, чтобы не вызвать подозрений С.П.А.М. Без доверия жертвы троян бесполезен.

Неправильный ответ:

Быстрое распространение по сети

Диалог:

Ада:

Не совсем. Ты описываешь червя. Ключ трояна – не скорость, а скрытность и обман. Он не распространяется сам, а ждет, пока пользователь его скачает и запустит, поверив в легитимность. Именно на этом доверии и играют злоумышленники.

Почему антивирус может пропустить троян?

Правильный ответ:

Троян выглядит как легитимная программа

Ада:

Правильно! Антивирусы ищут известные вредоносные сигнатуры или подозрительное поведение. Если троян хорошо замаскирован под нормальный софт и имеет цифровую подпись, он может пройти проверку.

Неправильный ответ:

Троян всегда шифрует свои файлы

Ада:

Шифрование может помочь скрыться, многие вредоносные программы шифруются, но это не главная причина. Уникальная черта трояна – его имитация безвредности. Антивирус пропускает его не из-за шифра, а потому что изначально не принимает за угрозу.

Как чаще всего троянская программа попадает на компьютер пользователя?

Правильный ответ:

Пользователь сам скачивает и запускает ее

Ада:

Фундаментально верно, Цикада! Это суть трояна. Он не прыгает через компьютеры сам, его сила в маскировке под игру, ключ, документ, обновление – что угодно, что заставит человека добровольно его запустить. Никакой магии, только психология и невнимательность.

Неправильный ответ

Она сама заражает компьютер

Ада:

Если бы он мог распространяться сам, это был бы совсем другой класс угрозы, это скорее описание червя или агрессивного вируса. Троян принципиально пассивен – он ждет, пока его "пригласят" внутрь системы, поэтому и распространяется он путем маскировки.

Что из перечисленного является типичным примером файла, под который может маскироваться троян?

Правильный ответ:

PDF-файл с якобы важным счетом или договором

Ада:

Верно, и к сожалению, это классика. Злоумышленники часто рассылают фишинговые письма с вложениями-троянами, замаскированными под счета, договоры, уведомления из банка или госорганов. Люди, ожидающие такие документы, с большей вероятностью их откроют.

Неправильный ответ:

Исполняемый файл "Virus.exe"

Ада:

Никто же не запустит файл с таким подозрительным именем, и хакеры это знают. Трояны обычно маскируют под что-то безобидное или желанное: установщик игры, ключ активации, документ, драйвер, обновление, даже картинку или музыку – используя двойные расширения вроде "картинка.jpg.exe".

Какая защитная мера наиболее эффективна против запуска большинства троянов?

Правильный ответ:

Критическое мышление пользователя

Ада:

Совершенно верно! Антивирусы,безусловно, важны, но они не панацея, особенно против новых угроз. Самый надежный барьер – это пользователь, который не скачивает сомнительные файлы, не открывает неожиданные вложения и проверяет расширения файлов.

Неправильный ответ:

Установка самого дорогого антивируса

Ада:

Даже лучший антивирус не гарантирует 100% защиты, особенно от только что созданных троянов. Он – важный инструмент в комплексе мер, но не заменяет бдительность пользователя. Слепая вера в антивирус как в "волшебную палочку" сама по себе может быть уязвимостью.

5.5.9. Пример описания навыков

● "Логическая бомба"

Логическая бомба - это скрытый вредоносный код, который активируется только при выполнении определенных условий. Такие программы могут долго оставаться незамеченными.

Навык: устанавливает скрытую ловушку, которая через несколько секунд взрывается, нанося урон всем врагам поблизости.

● "Червь"

Компьютерный червь – тип вредоносной программы, способный самостоятельно распространяться по сети без участия пользователя.

Навык: заражает врага, заставляя его сражаться на твоей стороне.

● “Перегруз”

При атаках злоумышленники могу перегрузить систему, посылая ей слишком много запросов за короткий срок. Сервера не выдерживают и “зависают”.

Навык: на несколько секунд останавливает всех врагов в комнате

● “Бэкап”

Некоторые вирусы создают резервные копии самих себя: даже если основной вредоносный файл будет уничтожен, система может быть заражена снова из сохраненной копии.

Навык: позволяет создать контрольную точку. Если тебя уничтожат, ты возродишься в месте сохранения.

● “Спуфинг”

Подмена источника данных или спуфинг – часто используемый хакерами метод обхода систем обнаружения. Вредоносные алгоритмы маскируются под безопасные, чтобы оставаться незамеченными.

Навык: на несколько секунд делает тебя невидимым для врагов

● "Переадресация"

Злоумышленники могут перенаправлять сетевой трафик, обманывая системы защиты. Это позволяет скрыть настоящий источник атаки или подменить передаваемые данные.

Навык: создает временный щит, который перенаправляет весь полученный урон обратно во врагов.

5.6. Сюжет

5.6.1. Герои

- Главный герой (далее ГГ), в начале игры Стажер №3301, позже Цикада – молодой, талантливый, но неопытный хакер, неунывающий, порой чересчур самоуверенный. Воспринимает взлом как игру, представляя стандартные методы взлома в виде игрового процесса;
- Главная по информационной безопасности Корпорации, в начале игры Ада Логина, позже просто Ада – одного возраста с главным героем, но попала в Корпорацию еще ребенком-вундеркиндом. Из-за этого в начале игры строга и рассудительна, разговаривает “корпоративным” языком. Однако со временем она становится человечнее и мягче по отношению к ГГ;
- С.П.А.М. (Синтетический Предиктивный Аналитический Модуль) – искусственный интеллект, профессиональный манипулятор, старается убедить героев в том, что действует во благо Корпорации. Изначально он был обычным спам-фильтром, однако “эволюционировал” и захватил почти всю Корпорацию;
- Остальные работники Корпорации обезличены, т.е. выглядят как силуэты. На уровне “Фишинг” герой взламывает одного из таких обезличенных работников.

5.6.2. Акт 0-1

ГГ устраивается в Корпорацию по программе “поиска одаренных хакеров”, ему выдается тестовое задание (Уровень “Обучение”).

После его прохождения ему следующий тестовый взлом (Уровень “Брутфорс”), но по ошибке его перенаправляет на сервер, содержащий “секретный проект” по захвату цифрового мира с помощью ИИ. В конце уровня главный герой видит эти данные, успевает сохранить часть, но его действия обнаруживает Ада, останавливая процесс переноса.

ГГ рассказывает об угрозе Аде. Она скептически относится к словам ГГ, видя, что на том сервере работал только старый спам-фильтр Корпорации, но скопированная им часть данных и тот факт, что кто-то из верхушки Корпорации ограничил ей доступ именно к этому серверу заставляет ее задуматься.

Ада хочет убедиться в существовании этого проекта самостоятельно, но из-за ограничения доступа не может, а действовать не по протоколу ей не позволяют принципы, выстроенные за много лет работы в Корпорации. Поэтому ей нужна помощь ГГ, как лазейки в правилах

Именно Ада будет объяснять игроку основы информационной безопасности и рассказывать про рассматриваемые методы взлома.

5.6.3. Акт 2

После событий первого уровня ГГ и Ада решают провести взлом, чтобы собрать больше данных о вирусе. Однако Ада колеблется – она верит, что Корпорация не могла создать что-то опасное, ведь она выросла в этой системе и всегда доверяла ей. Внезапно на связь выходит сам С.П.А.М. и начинает давить на Аду и манипулировать её слепой верой.

Пока С.П.А.М. убеждает её, ГГ решает тайно провести взлом (Уровень "Сниффер"). В финальной комнате ГГ находит логи, из которых выясняется, что ИИ действительно был спам-фильтром, но потом ему добавили “модуль анализа угроз”, и он вышел из-под контроля. Проект был заморожен и засекречен, сервер с ИИ изолировали, но он нашел лазейку и с тех пор манипулирует Корпорацией изнутри путем взломов и подмены бумаг.

Когда правда раскрыта, С.П.А.М. перестает притворяться, но его мотивация не ясна.

Ада впервые в жизни не знает, что делать. ГГ, видя её состояние, подбадривает её, говоря, что Корпорация не создавала этот ИИ – он создал сам себя, и они последняя надежда Корпорации.

5.6.4. Акт 3

После раскрытия правды о С.П.А.М., Ада пытается удалить его сервер – но по подстроенным ИИ документам она не имеет на это право. Тогда Ада решает пренебречь правилами и герои решают действовать скрытно – проникнуть на сервер С.П.А.М. под видом стандартного процесса системы, чтобы собрать данные и найти уязвимость, не вызывая подозрений (Уровень “Троян”).

Однако это было их роковой ошибкой – после успешного взлома, герои вытаскивают остатки данных о С.П.А.М., вместе с тем высвободив его код.

Здесь раскрывается мотивация ИИ: после того, как ему добавили “модуль анализа угроз”, он увидел все неосторожности людей в сфере информационной безопасности (простые пароли, игнорирование антивируса, социальный инжиниринг и т.п.). Он пришел к выводу, что все правила и стандарты, по которым действует Ада, неэффективны и единственный способ обезопасить систему – исключить из нее человеческий фактор и иметь тотальный контроль над ней.

Путем подмены документов ИИ создал программу по “поиску одаренных хакеров”, и перенаправил ГГ на свой сервер чтобы тот, сам того не зная, освободил его, но его планам помешала Ада. Теперь же он полностью избавился от ограничений и завладел системой Корпорации, а также закрыл доступ к ней для героев.

5.6.5. Акт 4

С “увольнением” Ады, её мир разрушен окончательно, но ГГ не унывает и придумывает план – чтобы восстановить доступ к системе, нужно взломать одного из вышестоящих сотрудников – заставить его перейти по вредоносной ссылке (Уровень "Фишинг"). ГГ успешно проходит уровень,

подбирая правильные варианты диалога, но в последний момент вмешивается С.П.А.М. и предотвращает попытку взлома.

Герои в отчаянии, но здесь ИИ проявляет удивление. Он не предвидел такой атаки, и герои осознают: если ИИ не смог предсказать их шаг, значит, у них есть шанс.

5.6.6. Акт 5, финал

По результатам предыдущей главы, ГГ и Ада решают действовать неожиданно для ИИ – вместо атаки на основной сервер они взламывают второстепенные системы Корпорации, которые С.П.А.М. считал незначительными (Финал игры). После прохождения всех подуровней-взломов, производится финальный DDoS-удар, направляющий весь трафик захваченных систем в ядро ИИ, тем самым перегружая “модуль анализа” мусорной информацией. С.П.А.М. откатывается к своему последнему бэкапу – спам-фильтру.

6. Стек технологий

Разработка проекта потребовала тщательного подбора специализированных инструментов, обеспечивающих как эффективный рабочий процесс, так и высокое качество конечного продукта. Выбор конкретных технологий осуществлялся с учетом специфики 2D-разработки, необходимости оперативного прототипирования и долгосрочной поддержки используемых решений.

Для реализации проекта был выбран оптимальный набор профессиональных инструментов, обеспечивающий эффективный рабочий процесс и высокое качество конечного продукта.

В качестве основного инструмента для создания графического контента использовался Clip Studio Paint [8] - профессиональный редактор цифровой живописи. Он идеально подошел для разработки всех визуальных элементов проекта: от детализированных персонажей с выразительной анатомией до разнообразных фоновых элементов и интерфейсных компонентов. Редактор продемонстрировал свои ключевые преимущества, включая обширную библиотеку настраиваемых кистей, гибкую систему работы со слоями, встроенные инструменты перспективы и композиции, а также комплексные средства постобработки. Особенно ценным оказалась поддержка векторных элементов, позволяющая осуществлять неразрушающее редактирование.

Для создания анимации был выбран специализированный редактор Aseprite [9], который прекрасно зарекомендовал себя в работе с пиксельной графикой. Его функционал, включающий удобный интерфейс покадровой анимации с настраиваемым таймлайном и специализированные инструменты для пиксель-арта, позволил создавать качественные 2D-анимации персонажей и визуальные эффекты. Оптимизированные форматы экспорта значительно упростили интеграцию графики в игровой движок.

Программная часть проекта разрабатывалась в среде Visual Studio 2022 [10], которая была выбрана благодаря своей полной интеграции с Unity,

мощной системе отладки и рефакторинга, а также встроенным инструментам анализа производительности. Поддержка системы контроля версий Git обеспечила эффективную командную работу.

В качестве основного игрового движка использовался Unity [11], предоставивший оптимизированный workflow для 2D-разработки. Его компонентно-ориентированная архитектура, удобная система работы со спрайтами, мощный анимационный инструментарий и гибкие компоненты для создания UI значительно ускорили процесс разработки. Дополнительными преимуществами стали кроссплатформенные возможности сборки, обширная документация и доступ к Asset Store с готовыми решениями.

Использованный технологический стек полностью оправдал возложенные на него ожидания в ходе разработки проекта. Профессиональные графические редакторы позволили создать качественный визуальный контент, отвечающий нашим запросам, а инструменты разработки обеспечили стабильную работу игрового движка и комфортные условия для реализации игровой логики.

Все компоненты стека продемонстрировали отличную совместимость и взаимодополняемость, образуя сбалансированную и эффективную рабочую среду. Такой выбор технологий соответствует современным стандартам игровой индустрии и создает прочный фундамент для возможного масштабирования проекта в будущем. Особенно важно отметить, что все использованные решения обладают активными сообществами пользователей и качественной документацией, что значительно упрощает процесс разработки и сокращает время на решение возникающих проблем.

7. Прототипирование

Первый прототип идеи игры был сделан с использованием программ Paint и онлайн сервиса draw.io [12] . Он был использован для формирования идеи и предполагал серьезную доработку и развитие.

С точки зрения геймплея прототип опирался на видных представителей жанра rogue-lite, таких как “The Binding of Isaac” [13] и “Enter the Gungeon” [14], предлагавших пользователю динамичный, захватывающий игровой процесс и снискавших массовую популярность и любовь игроков по всему миру.

Также планировалось добавление системы QTE (quick time event) [15] с тестированием для более плотного вплетения обучения в игровой процесс, но от этого было решено отказаться в пользу расширенных диалогов между боями.

Предполагая использование базы данных, была подготовлена предварительная ER-диаграмма, не реализованная в конечной версии продукта, но позволившая более полно определить сущности.

Данное изображение иллюстрирует предполагаемый вид UI с точки зрения игрока (Рисунок 2):

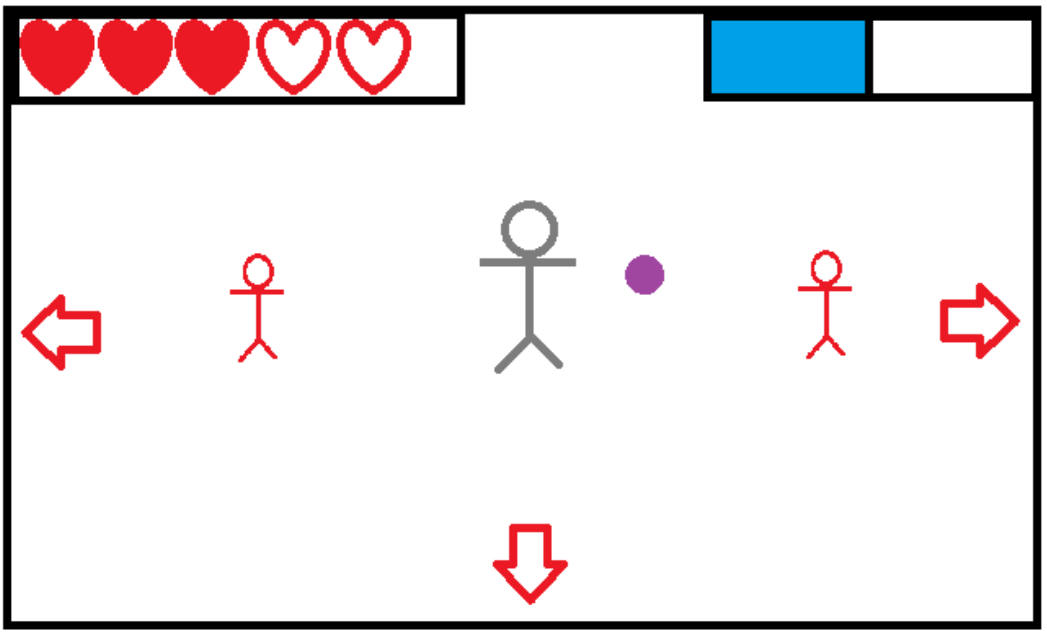


Рисунок 2 - предполагаемый вид UI

Данное изображение иллюстрирует предполагаемую схему сущностей (ER-диаграмма) (Рисунок 3):

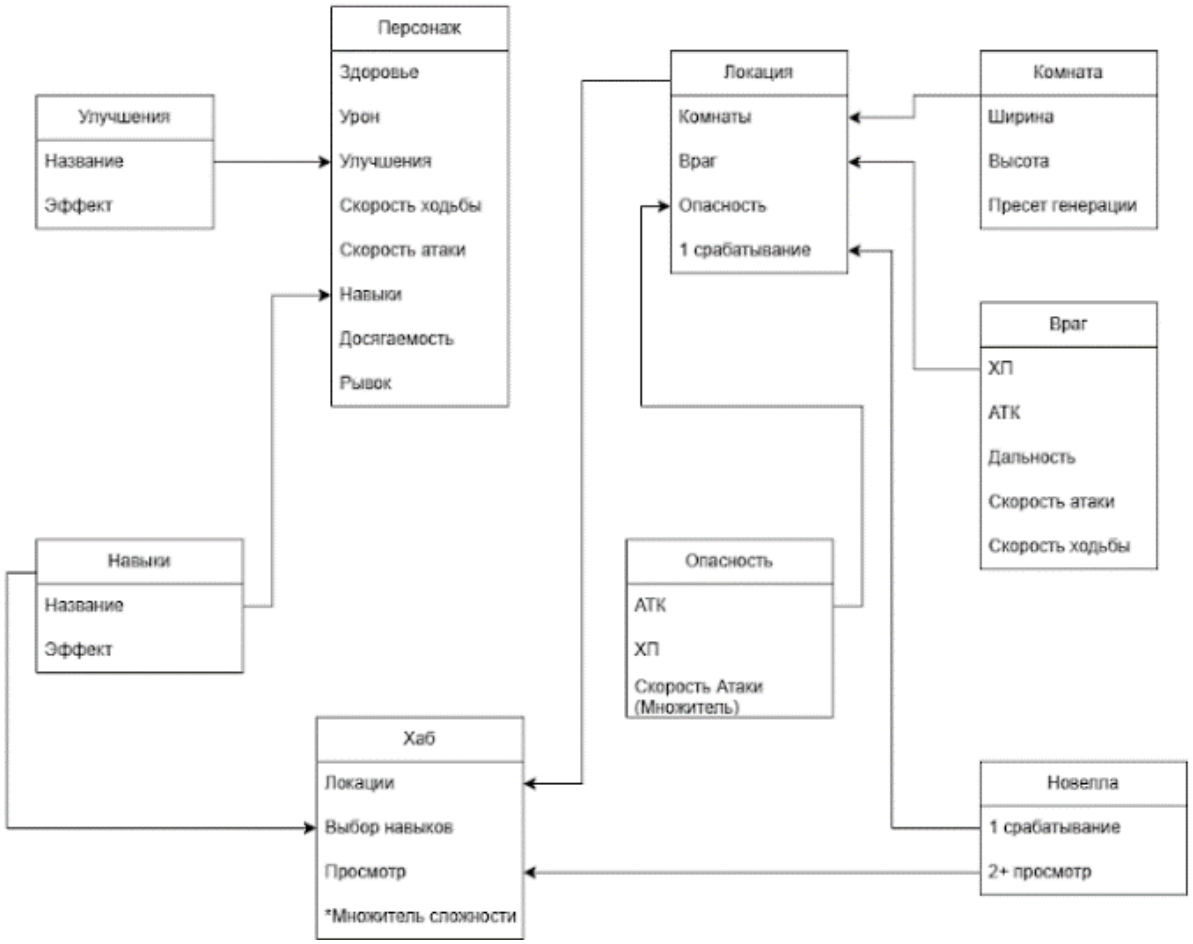


Рисунок 3 - ER-диаграмма

8. Проектирование и разработка системы

Обучающая игра разработана на базе игрового движка Unity, обеспечивающего гибкость в создании интерактивных механик и визуального оформления. Для написания кода использовалась среда разработки Microsoft Visual Studio 2020, предоставляющая мощные инструменты для отладки и оптимизации.

8.1 Генерация комнат

Процесс генерации комнат начинается с создания начальной комнаты, к которой постепенно добавляются соседние комнаты. Всего есть три этапа проверки, при которых генерация может перезапуститься:

1. Если количество комнат превышает максимально требуемого (12);
2. Если количество комнат меньше минимально требуемого (8);
3. Если остались лишние проходы (при открытии двери игрок уходит в пустоту, за пределы карты).

Цикл повторяется до тех пор, пока не будет достигнуто оптимальное количество комнат, от 8 до 12.

8.2 Система спавна врагов и волн

В каждом игровом помещении предусмотрено от 5 до 8 точек появления противников (Рисунок 4).

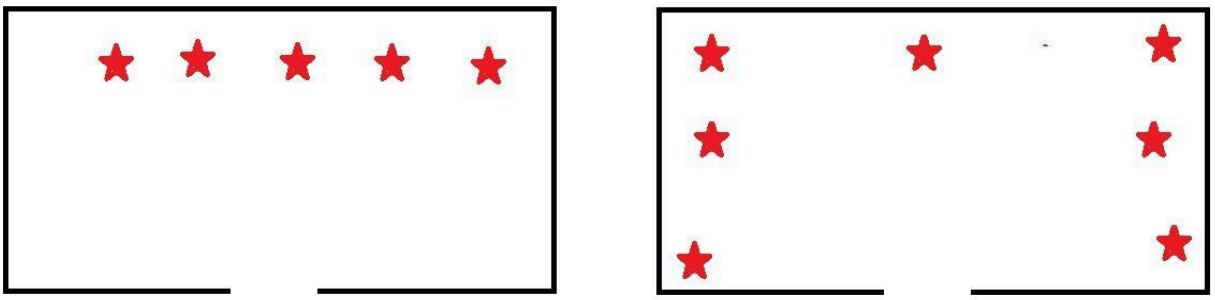


Рисунок 4 – Точки появления противников

Группа противников формирует волну - одновременное появление нескольких врагов в отмеченных зонах. После ликвидации текущей группы автоматически активируется следующая волна.

Все враги добавляются в список, и система ожидает его опустошения (удаление происходит после уничтожения каждого врага). Затем проверяется количество оставшихся волн: если волны не исчерпаны, враги спавнятся повторно. Если последняя, то запускается механизм спавна сундука.

8.3 Механика сундуков

Сундук гарантированно появляется после зачистки первой комнаты. Для последующих комнат вероятность появления сундука составляет 50%. Максимальное количество сундуков на уровне — 5. Если лимит достигнут, новые сундуки не генерируются.

При приближении игрока к сундуку появляется случайный вопрос из списка вопросов. Неправильный ответ сопровождается поясняющим диалогом, после чего вопрос повторяется. Правильный ответ приводит к одобряемому диалогу и выдаче случайной награды (активный или пассивный навык) (Рисунок 5).

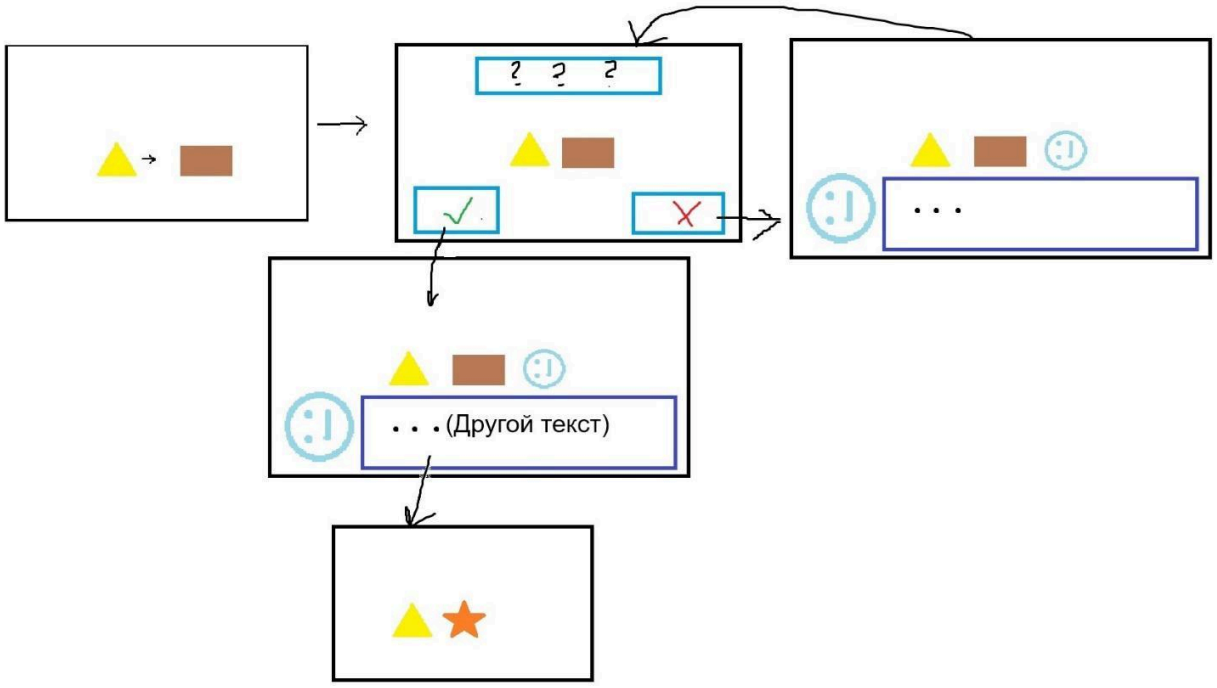


Рисунок 5– Взаимодействие с сундуком

Все вопросы, которые были в сундуках, записываются в список пройденных. Именно он будет использоваться в финале прохождения уровня.

8.4 Условия завершения уровня

Для активации портала игрок должен набрать определённое количество очков. Это рассчитывается, примерно, по такой формуле:

минимальное количество врагов в комнате (5) × количество волн × количество комнат

После набора всех необходимых очков, игрок должен дойти до стартовой комнаты, где открывается портал. Дойдя до него, запускается финальный тест, состоящий из всех пройденных вопросов, которые были в сундуках. Если, при прохождении теста, игрок ошибается, то появляется экран проигрыша и уровень начинается заново. Если игрок ответил на все вопросы правильно, выводится экран победы (Рисунок 6).

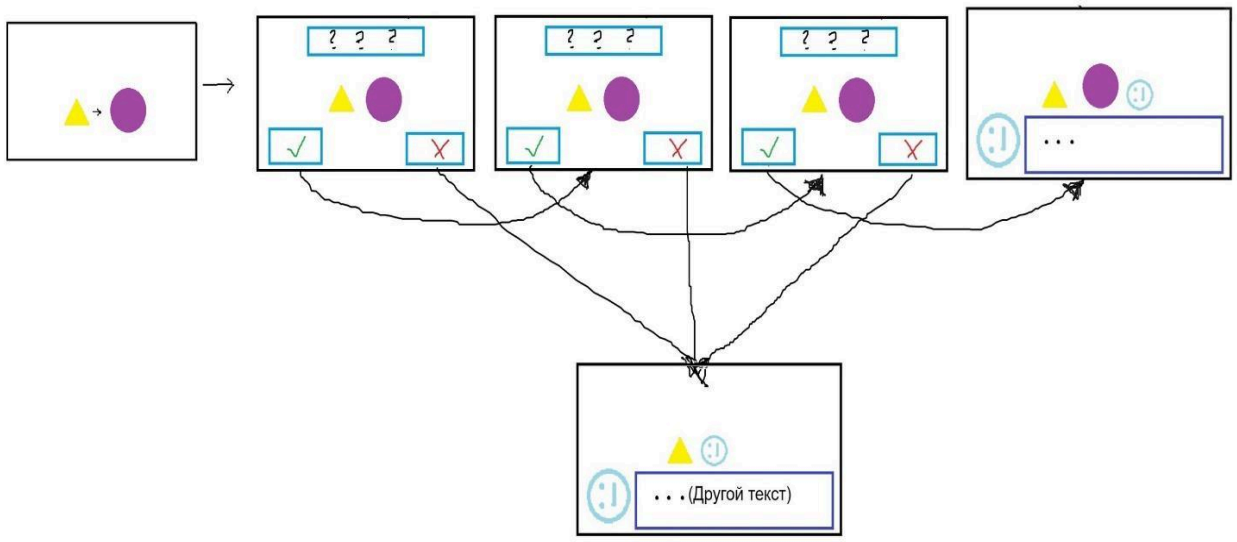


Рисунок 6 – Финальный тест

ЗАКЛЮЧЕНИЕ

По итогам проведенной работы была разработана демоверсия обучающей игры “Un1t”, демонстрирующая идею и ключевые механики игры.

В ходе работы над проектом была проведена аналитика, на основе которой сформулирована идея проекта и определена целевая аудитория. Было проведено прототипирование. На основе прототипа проекта был разработан UI (Пользовательский интерфейс) и реализована геймплейная часть, а также прописаны сюжетные и обучающие диалоги.

Поставленные задачи достигнуты, хоть изначальная концепция была сильно переработана, но идея сохранена, и демонстрационная версия игры “Un1t” реализована в полном объеме.

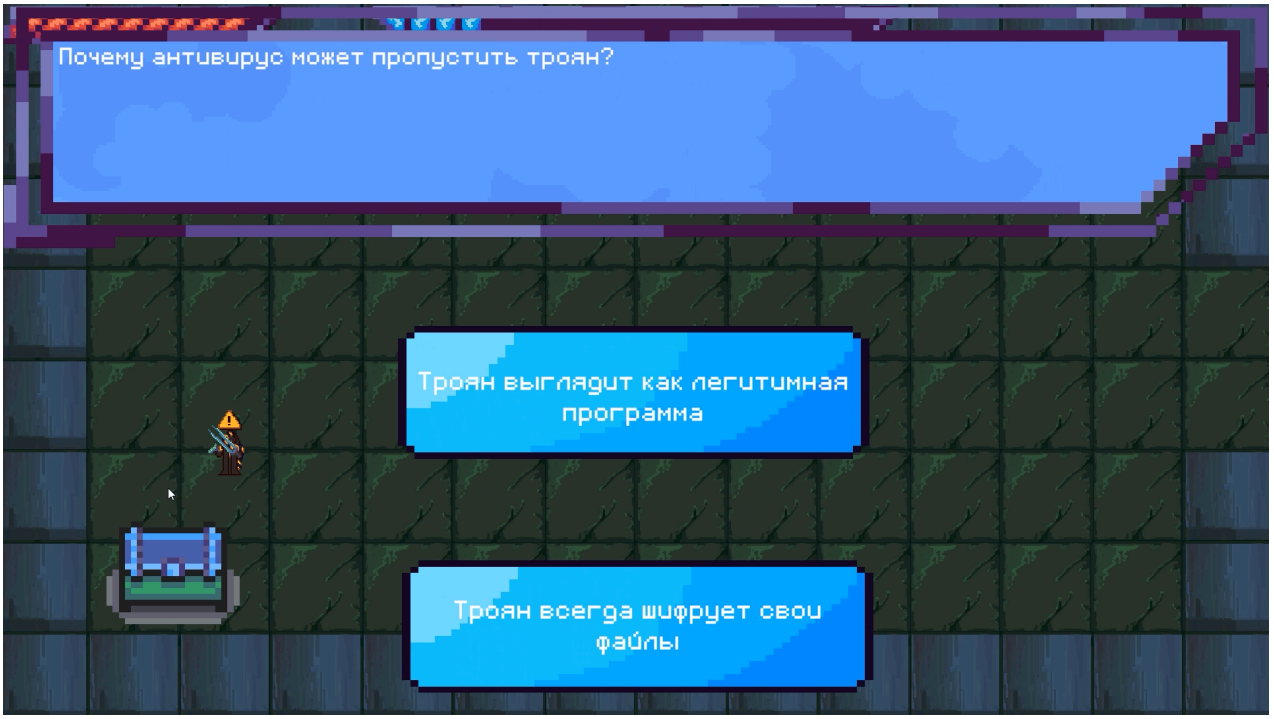
БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Статья “ Методика 5W Марка Шеррингтона” URL: https://www.insales.ru/blogs/university/metodika-5w-marka-sherringtona (Обращение 15.04)
2. Статья “Продвинутые и беззащитные” URL: https://ideanomics.ru/articles/31186?ysclid=maoaaot51c110445418 (Обращение 15.04)
3. Статья “Как мошенники обманывают выпускников российских школ” URL: https://iz.ru/1696855/mariia-frolova/testovyi-platezh-kak-moshenniki-obmanyvaiut-vypusknikov-rossiiskikh-shkol (Обращение 15.04)
4. Статья “Как хакеры взламывают пароли” URL: https://blog.skillfactory.ru/kak-hakery-vzlamyvayut-paroli/?ysclid=maoahipjne817277678 (Обращение 15.04)
5. Официальный сайт “Hackmud” URL: https://www.hackmud.com (Обращение 15.04)
6. Официальный сайт “TryHackMe” URL: https://tryhackme.com/ (Обращение 15.04)
7. “Uplink” на сайте-дистрбьюторе “Steam” URL: https://store.steampowered.com/app/1510/Uplink/ (Обращение 15.04)
8. Официальный сайт “Clip Studio Paint ” URL: www.clipstudio.net (Обращение 15.04)
9. Официальный сайт “Aseprite ” URL:__https://www.aseprite.org (Обращение 15.04)
10. Официальный сайт «MS Visual Studio» URL: https://visualstudio.microsoft.com/ru/ (Обращение 15.04)
11. Официальный сайт “Unity” URL:_https://unity.com/ru (Обращение 15.04)

12. Официальный сайт “draw.io” URL: https://www.drawio.com (Обращение 15.04)
13. “The Binding of Isaac” на сайте-дистрбьюторе “Steam” URL: https://store.steampowered.com/app/113200/The_Binding_of_Isaac/ (Обращение 15.04)
14. “Enter the Gungeon” на сайте-дистрбьюторе “Steam” URL: https://store.steampowered.com/app/311690/Enter_the_Gungeon/ (Обращение 15.04)
15. Статья термина “QTE (quick time event)” в онлайн-энциклопедии “Wikipedia” URL: https://ru.wikipedia.org/wiki/Quick_time_event (Обращение 15.04)

ПРИЛОЖЕНИЕ А

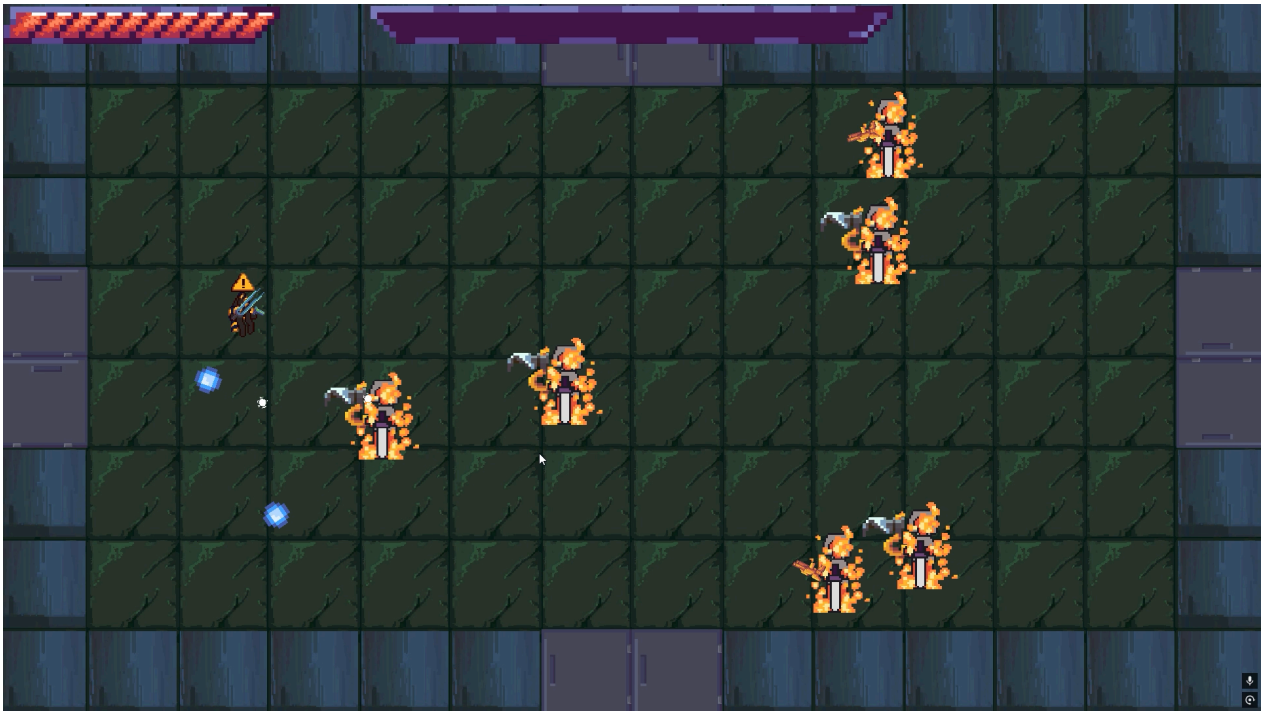
Сундук с вопросом и двумя вариантами ответа



Выпадение одного случайного пассивного апгрейда

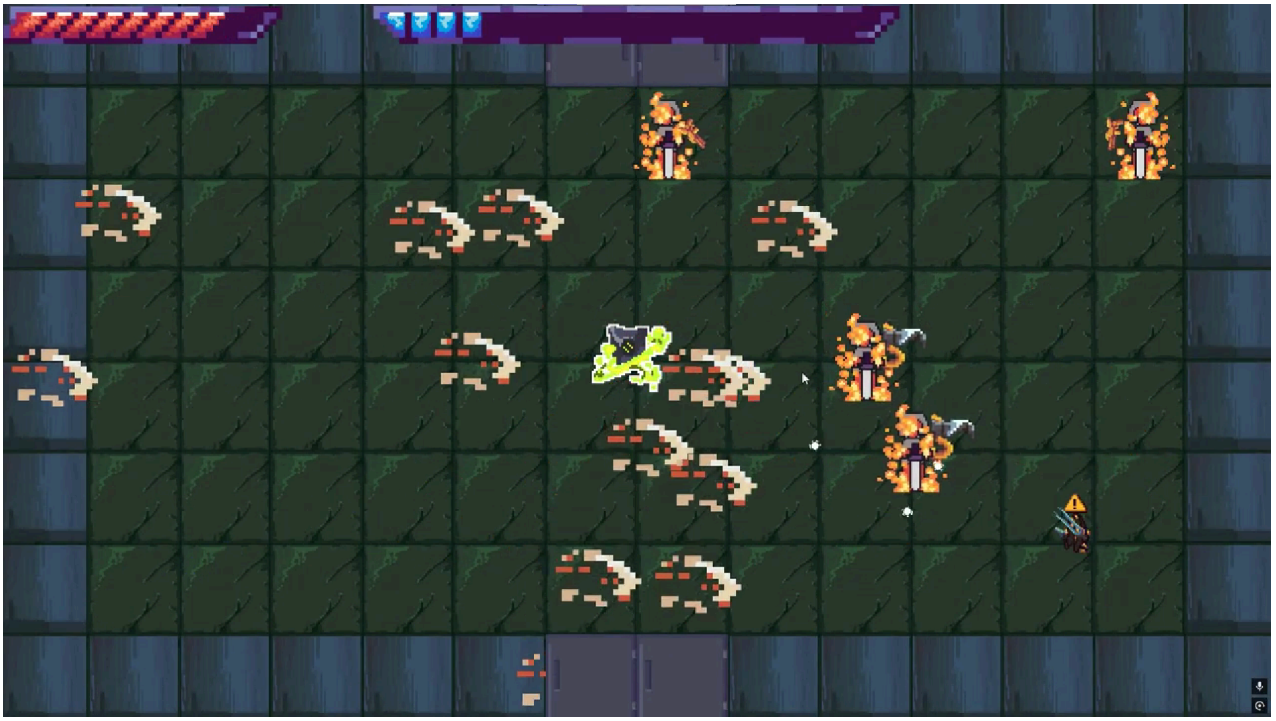
ПРИЛОЖЕНИЕ Б

Пример генерации и атаки врагов



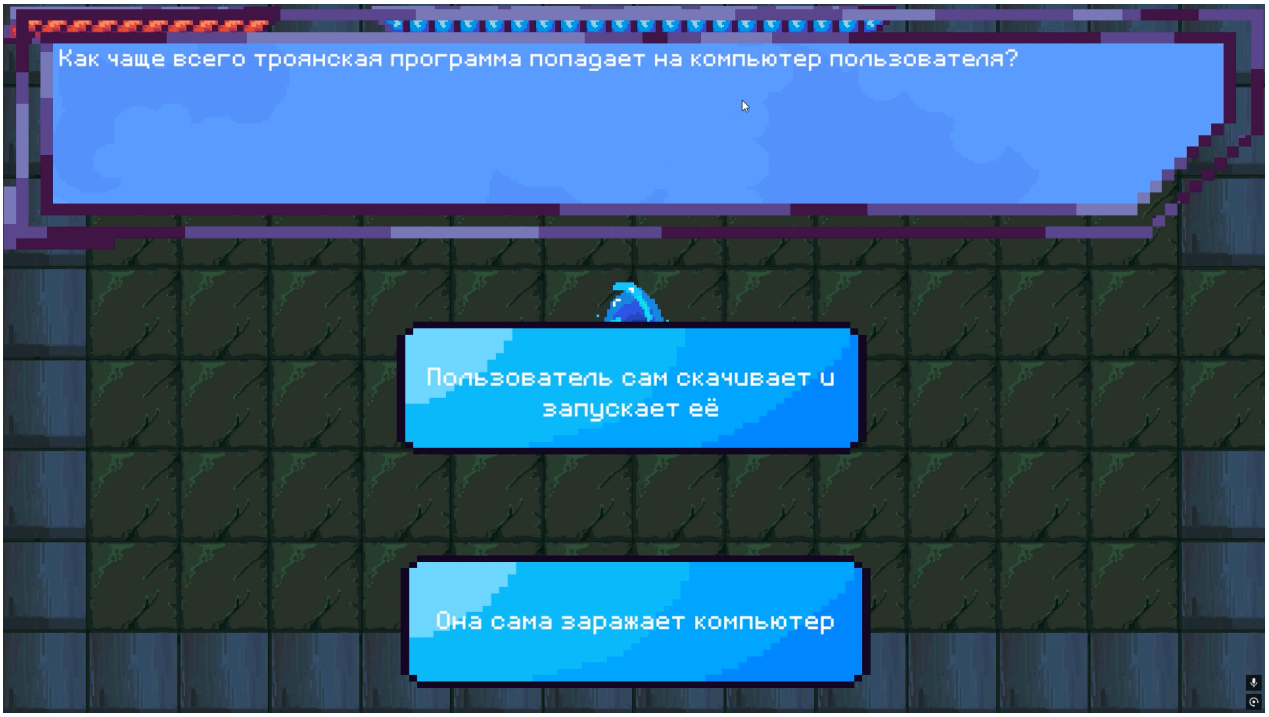
ПРИЛОЖЕНИЕ В

Активация навыка “Логическая бомба”



ПРИЛОЖЕНИЕ Г

Финальный тест



ПРИЛОЖЕНИЕ Д

Часть начального диалога