

Мирза Мурат Юнусович

старший преподаватель

Шишхова Аминат Пиимафовна

ассистент

Тутаришев Альберт Казбекович

старший преподаватель

Алиева Ламан Фаиговна

студентка

Кононенко Владислава Васильевна

студентка

ФГБОУ ВО «Адыгейский государственный университет»

г. Майкоп, Республика Адыгея

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В ОНЛАЙН-ИГРАХ: КАК ПОДРОСТКОВ ВОВЛЕКАЮТ В МОШЕННИЧЕСТВО

Аннотация: в статье рассмотрена проблема широкого распространения киберпреступлений, связанных с подростками, которые, не имея достаточных знаний в области цифровой грамотности и распознавании манипуляции, попадают под большой риск вовлеченности в преступные схемы мошенниками, использующих их интересы к онлайн-играм и атрибутам.

Ключевые слова: онлайн-игра, психологическое воздействие, преступные схемы, игровые бонусы, виртуальное общение, «прокачка» аккаунтов, игровые валюты, цифровая грамотность.

На сегодняшний день развитие научно-технического прогресса коснулось буквально всех слоев общества. Невозможно себе представить любое направление деятельности человека без использования компьютеров, интернета, всевозможных мессенджеров. Онлайн-среда стала вполне привычным явлением и даже некой обыденностью: здесь происходят знакомства, люди общаются, обмениваются информацией, проводят деловые встречи, обучаются, проводят досуг и все это происходит в сети и занимает значительную часть времени. Дети так же, как

и взрослые, являются завсегдатаями онлайн-среды, и даже в большей степени, и одной из причин длительного времяпровождения у детей являются онлайн-игры, которые с легкой руки взрослых с ранних лет входят в их жизнь, при этом не отдавая себе отчет в том, что вместе с безграничными возможностями приобретаются и серьезные риски. В последние годы очень широкое распространение получили киберпреступления, поскольку злоумышленники нашли довольно малозатратный путь к обогащению используя детей, их интересы к онлайн-играм и всем атрибутам, присущим играм: игровые бонусы, редкие дополнения, бесплатные обновления, «прокачки» аккаунтов. При этом они используют довольно простые и незамысловатые схемы, что и позволяет добиваться успеха не вызывая подозрений, входя в доверие через всевозможные комплименты и похвалу, красивые слова, поддержку в ведении игры, в некоторых случаях помогая проходить сложные для детей уровни. Дальше в обмен на обещания дальнейшего игрового развития, мошенники получают у детей доступ к личным данным, аккаунтам и, самое главное, пытаются получить банковские средства родителей и довольно часто это им удается. Подростки попадают под психологическое воздействие поскольку не осознают возможных проблем от общения с незнакомыми людьми в интернете, в силу недостаточности знаний в области цифровой грамотности и неумения распознавать манипуляции.

Очень часто подростки рассказывали о случаях, когда им приходили сообщения с различными предложениями, например перейти в другие мессенджеры, двигаться дальше используя ссылки, получить дополнительные бонусы в обмен на личные данные, получение игровых валют, что при отсутствии прямой угрозы или опасности, они воспринимали их как часть игрового общения или стратегию командной игры. В понимании подростков виртуальное общение не вызывает опасений, поскольку есть «кнопка», которой всегда можно прервать общение, отключить, выйти. Дети в силу своей неопытности слишком доверчивы и легко поддаются внушению, чем злоумышленники и пользуются, маскируясь под таких же игроков, «друзей в чатах», членов команды в играх.

В связи с этим важной частью работы с подростками является не только формирование знаний в области цифровой грамотности, но и навыков безопасного поведения в интернете, вооружить детей знаниями по цифровой и финансовой грамотности, познакомить с часто используемыми схемами мошенничества в онлайн-играх.

В данной работе мы обозначили ряд задач:

- описать и показать одну из самых распространенных схем мошенничества в онлайн-играх;
- объяснить детям, почему опасно доверять незнакомым людям в интернете;
- обратить внимание на важность не передавать никому и держать в сохранности свои личные данные и личные данные других;
- рассказать о возможных последствиях, наступающих после передачи информации посторонним лицам;
- выделить, как важно обращаться к взрослым в случае, если заметили подозрительные действия и манипуляции;
- повысить внимательность и разборчивость при общении в социальной среде.

В рамках данного проекта нами был создан видеоролик продолжительностью 3 минуты, ссылка: <https://rutube.ru/video/3509ad0bf24df06d88ff0d6573b7baa2/?r=a/>

В основе сюжета видеоролика лежит переписка, максимально приближенная к реальным ситуациям, с которыми могут столкнуться дети. Главный герой играет в ROBLOX, где он знакомится с другим игроком. Этот игрок дружелюбен в общении и помогает ребенку. Почувствовав более открытое отношение к себе, он предлагает перейти в стороннюю социальную сеть для «удобного общения». Мошенник входит в доверие ребенка постоянно расхваливая, подбадривая его, говоря ему, что он очень продвинутый, особенный и хорошо играет, предлагает ребенку игровую валюту «робуксы». Но для получения доступа к ним, мошеннику, якобы, нужно подтверждение аккаунта, и чтобы осуществить перевод «робуксов» необходимо произвести привязку банковской карты родителя и просит

прислать ее фотографию. Он приводит «убедительные» аргументы о баснословных бонусах, высоком рейтинге и прочих благах, но при этом предупреждает, чтобы ребенок не сообщал родителям, по крайней мере пока не получит высокий статус или огромную прибыль, тогда это будет сюрпризом для них. Кульминацией становится момент, когда ребёнок передаёт данные и его блокируют. После этого показываются последствия подобных действий: эмоциональное переживание героя, чувство страха и осознание ошибки. При создании ролика мы старались использовать понятный детям формат, реалистичность переписки, простой язык и ситуацию.

Целевой аудиторией нашего проекта выступают дети и подростки 10–12 лет, которые активно пользуются онлайн-играми, игровыми платформами и мессенджерами.

После завершения всех подготовительных работ, мы посетили две учебные организации: ГБОУ РА «Адыгейская республиканская гимназия №1» и в МБОУ «Эколого-биологический лицей №35». В реализации проекта приняло участие 74 ребёнка из 4 классов: 42 школьника в возрасте 10 лет, 29 школьников в возрасте 11 лет и 3 школьника 12 лет.

Перед тем, как показать видеоролик, с детьми была проведена ознакомительная беседа, в которой мы поинтересовались: в какие игры они играют, сталкивались ли они или их друзья с подозрительными сообщениями и знают ли о случаях обмана в интернете.

Многие из детей активно включались в процесс и рассказывали свои истории: кому-то предлагали бесплатные «робуксы», кого-то просили перейти по ссылке, а нескольким детям уже писали незнакомцы в игровых чатах. Также приводились случаи, когда предлагали бесплатные «скины» за пароль от аккаунта, в следствии чего остались без них.

До просмотра видеоролика участникам было задано 5 вопросов на определение уровня знаний и подготовленности о способах ведения онлайн игр, с однозначным ответом «да» или «нет».

1. Считаете ли вы безопасным тот факт, что во время игры приходится общаться, объединяться в команды с совершенно незнакомыми людьми?
2. Возможна ли в ходе игры ситуация, когда возникает необходимость переходить в другой чат по просьбе партнера по игре или команды?
3. Насколько достоверна возможность приобретение в процессе игры за какие-нибудь дополнительные действия бесплатных бонусов или игровой валюты?
4. Возможны ли ситуации в играх, когда для успешного прохождения уровня, приобретения дополнительных усовершенствований или какого-либо сохранения необходимо внести денежные средства используя для этого данные аккаунта или банковской карты?
5. Существует ли вероятность возникновения ситуаций во время игр, когда вам будет необходима помощь или вмешательство взрослых?

После просмотра и обсуждения сюжета и проблемы, затронутой в видеоролике, детям были повторно заданы те же вопросы. До просмотра видеоролика часть детей воспринимала общение с незнакомцами в игре как обычную ситуацию, одним из способов комплектации команд или отбора соперников и не считала переход в сторонние мессенджеры чем-то опасным. Некоторые участники были уверены, что бесплатные игровые бонусы действительно можно получать от других игроков или за дополнительный игровой прогресс. После просмотра ролика и обсуждения, мы обратили внимание, что дети стали заметно осторожнее в ответах. Во время повторной беседы многие уже самостоятельно объясняли, почему нельзя сообщать личные данные и переходить по подозрительным ссылкам.

Результаты анкетирования показали следующие изменения в ответах детей до и после предшествующих разъяснений:

- количество детей, понимающих опасность общения с незнакомцами в игре, увеличилось с 44% до 59%;
- осведомлённость о рисках перехода в сторонние мессенджеры выросла с 42% до 64%;

– число участников, понимающих опасность «бесплатных бонусов», увеличилось с 48% до 70%;

– понимание недопустимости передачи данных аккаунта и банковской карты выросло с 63% до 92%;

– готовых обратиться за помощью к взрослым увеличилось с 58% до 80%.

Во время обсуждения, после просмотра видео, дети стали задавать больше вопросов о защите аккаунтов и способах распознавания обмана. Многие эмоционально реагировали на финал видеоролика, обсуждали поступки героя и говорили, что будут внимательнее относиться к подобным сообщениям в играх.

В результате проведенной работы, мы обратили внимание, что тема киберпреступлений и интернет-безопасности вызывает у детей интерес и требует регулярного обсуждения. Несмотря на активное пользование цифровыми технологиями, мы отметили, что многие школьники еще недостаточно понимают каким образом действуют мошенники, какие последствия могут нести передача личных данных, какие действия предпринимать при обнаружении манипуляций со стороны злоумышленников. Созданный видеоролик позволил в доступной форме объяснить детям основные правила безопасного поведения в интернете и показать возможные реальные риски от общения с незнакомыми в онлайн-играх.

Практическая часть нашего проекта подтвердила эффективность донесения информации через визуальный формат. Интерес детей к возможным проблемам и рискам, связанным с онлайн-играми и онлайн-средой значительно вырос, что позволит им в дальнейшем внимательнее относиться к вопросам цифровой безопасности.

Список литературы

1. Собкин В.С. Подросток в социальных сетях: к вопросу о социально-психологическом самочувствии / В.С. Собкин, А.В. Федотова // Национальный психологический журнал. – 2018. – №3 (31). – С. 23–36. DOI 10.11621/npj.2018.0303. EDN YPELJR

2. Влияние социальных сетей на подростков. – URL:
<https://kopilkaurokov.ru/vneurochka/prochee/uchebnyi-proekt-vliianiie-sotsialnykh-sietiei-na-podrostkov> (дата обращения: 10.07.2026).