14.35.00

Информационная безопасность при использовании видеоигр

Николаева М.О.
Челябинский институт развития профессионального образования (ГБУ ДПО ЧИРПО), г. Челябинск, Российская Федерация
ORCID: https://orcid.org/0009-0003-7198-9995
e-mail: nikolaeva-15@bk.ru

Селютин А.А.
Челябинский институт развития профессионального образования (ГБУ ДПО ЧИРПО), г. Челябинск, Российская Федерация
ORCID: https://orcid.org/0000-0002-0575-9521
e-mail: alexsell@mail.ru

Статья посвящена информационной безопасности в ходе игрового онлайн-процесса. Основой статьи послужили результаты онлайн-опроса, в котором приняли участие 156 респондентов. Анализ опроса осуществлялся с разбивкой на три категории: возраст, гендер, занятость). Вопросы касались актуальных на сегодняшний день проблем нарушения информационной безопасности, связанных в первую очередь с человеческим фактором. Анализ ответов опрошенных осуществлялся в процентном соотношении с определением удельной доли. Авторы приходят к выводам о степени подготовки опрошенных к противодействию мошенническим действиям в компьютерных играх, а также о необходимости корректировки обучающих компонентов, связанных с приобретением навыков и умений информационной безопасности. Исследователи особо отмечают разницу в восприятии собственной защищенности в видеоиграх в зависимости от возраста, гендера и занятости респондента, указывая на значительную долю осторожности респондентов старшего возраста и на большую беспечность более молодого поколения пользователей компьютерных игр. Результаты опроса и выводы, сделанные на основании анализа, могут использоваться для формирования комплекса профилактических мероприятий, направленных на купирование угроз киберпреступности, а также на снижение рисков деструктивных проявлений при коммуникации в интернет-пространстве.

Ключевые слова: компьютерная игра, информационная безопасность, опрос, алгоритм, защита, персональные данные.

Для цитаты: *Николаева М.О., Селютин А.А.* Информационная безопасность при использовании видеоигр // Цифровая гуманитаристика и технологии в образовании (DHTE 2023): сб. статей IV Международной научно-практической конференции. 16–17 ноября 2023 г. / Под ред.

В.В. Рубцова, М.Г. Сороковой, Н.П. Радчиковой. М.: Издательство ФГБОУ ВО МГППУ, 2023. 513–523 с.

Введение

Компьютерные игры стали неотъемлемой частью нашего существования. С каждым годом количество пользователей, играющих в онлайн-игры, увеличивается, а виртуальные игры становятся одним из ключевых трендов интернет-активности. При этом по-прежнему актуальным остается вопрос информационной безопасности при осуществлении игрового процесса, поскольку компьютерные игры остаются чуть ли не единственным интернет-ресурсом, сохраняющим максимальные условия анонимности при условии активной интеракции, что создает благоприятные условия для различного рода мошеннических действий. Г.В. Семеко отмечает, что рейтинг глобальных рисков ВЭФ включает киберпреступность в первую пятерку, учитывая развитие киберугроз и приобретение киберпреступностью все более сложного и транснационального характера [4]. А.В. Кухаркин обращает внимание на то, что в России на правительственном уровне понимают возрастающую опасность нелигитимных киберагрессивных действий в цифровых сетях и разрабатывают механизмы противодействия [2]. Так, например, на правовом уровне защита персональных данных и персональной информации обеспечивается законами (Федеральный закон № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» и Федеральный закон № 152-ФЗ от 27.07.2006 г. «О персональных данных»). Однако между разработкой механизмов, их реализацией на практике и изменением сознания людей, стремящимся использовать механизмы профилактики и противодействия деструктивным проявлениям в виртуальном пространстве находится большая пропасть. П. Житнюк и А. Смирнов приводят простые примеры социальной инженерии и влияния человеческого фактора, позволяющие злоумышленникам обойти даже высокотехнологичную защиту персональных данных [1]. Наконец, А.Л. Осипенко и В.С. Соловьев подтверждают, что правонарушения с применением информационных технологий по отношению к несовершеннолетним занимают особое место [3]. При этом мы понимаем, что несовершеннолетние подростки являются основными пользователями компьютерных игр, что автоматически формирует целевую аудиторию в едином виртуальном пространстве, потенциально уязвимую для рисков деструктивного поведения мошенников. Таким образом, мы полагаем, что проблема информационной безопасности виртуального игрового процесса должна быть

исследована не только с точки зрения внутриигровых механизмов защиты при помощи программного обеспечения, но также и с точки зрения понимания пользователями компьютерных игр принципов, правил и алгоритмов информационной безопасности, чтобы исключить возможность применения социальной инженерии или не стать жертвой человеческого фактора.

Основной целью исследования является осознание степени нарушения правил информационной безопасности пользователями компьютерных игр, а также выявление проблемных точек, которые позволяют мошенникам пользоваться доверчивостью пользователей онлайн-игр.

Методы

Материалом исследования послужил опрос, который проводился в мае 2023 года посредством форм Google. В рамках опроса пользователям разных возрастов было предложено ответить на ряд вопросов, связанных с информационной безопасностью в процессе прохождения компьютерных игр. Общее количество опрошенных – 156 человек. Опрос проводился среди жителей города Челябинска и Челябинской области. Опросная методика предполагала анонимность предоставления результатов, в качестве персональных данных указывались лишь возрастная категория, гендер и род занятости. Опрос состоял из двух блоков: первый блок состоял из вопросов, касающихся информационной безопасности при использовании компьютерных игр, второй блок состоял из вопросов, затрагивающих социально-психологические аспекты игрового процесса. В данной работе мы остановимся только на анализе блока «Информационная безопасность».

Результаты

При анализе ответов на вопрос «Как избежать попадания на страницы поддельных продавцов компьютерных игр или игровых предметов?» выяснилось, что наиболее уязвимой группой пользователей являются люди старше 35 лет, более 50 % которых затрудняются с вариантом выбора ответа, а наиболее защищенными являются подростки до 18 лет, отмечающие варианты ответа со 100 % вероятностью. По гендерному признаку мужчины на 5–15 % компетентнее женщин в случае избежания риска попадания на страницы поддельных продавцов, и такое же превосходство в значениях демонстрируют студенты по отношению к уже работающим опрошенным.

В соответствии с результатами ответов большинство опрошенных не обновляют антивирусное обеспечение. По частотности обновления рекордсмены распределились следующим образом:
– раз в неделю – младше 18 лет (25 % опрошенных этого возраста);
– раз в месяц – от 23 до 35 лет (32 % опрошенных этого возраста);
– раз в год – от 18 до 23 лет (23 % опрошенных этого возраста).

Мужчины более небрежно относятся к обновлению антивирусного обеспечения (45 % опрошенных мужчин и 35 % опрошенных женщин не обновляют обеспечение). При этом треть опрошенных мужчин и женщин производят соответствующее обновление раз в месяц. Работающие опрошенные демонстрируют большую активность в обновлении антивирусного обеспечения, чем студенческая молодежь: 34 % работающих не обновляют обеспечение, при этом 50 % студентов ПОО и 37 % студентов вузов подтвердили отсутствие обновлений. Среди обновляющих антивирусное обеспечение превалируют ответы «раз в месяц» и «раз в год».

Большая часть опрошенных подтверждает, что их игровой аккаунт ни разу не был взломан или украден. При этом большинство подростков младше 18 лет предпочитают удалить игру с персонального устройства при возникновении подобной проблемы (25 %), студенческая молодежь в возрасте 18–23 лет предпочитает менять логин и пароль самостоятельно (29 %), работающая молодежь в возрасте 23–35 лет склоняется к обращению в техподдержку (13 %) или самостоятельной смене логина и пароля (13 %), а люди в возрасте старше 35 лет преимущественно обращаются в техподдержку (43 %). Мужчины, как и женщины, предпочитают обращаться в техподдержку или менять логин и пароль самостоятельно. Однако среди женщин отмечается большая доля бездействия (9 % женщин отметили, что ничего не стали делать, по сравнению с 2 % мужчин). Студенты ПОО полностью удаляют игру с устройства (11 %) или ничего не делают (17 %), студенты вузов склонны менять логин или пароль самостоятельно (30 %), а работающие опрошенные предпочитают обращаться в техподдержку (24 %).

Опрос показал, что чем старше возраст человека, тем он испытывает большие затруднения с алгоритмом защиты от вредоносных программ. Так, затруднились определить алгоритм защиты своего компьютера 36 % опрошенных в возрасте старше 35 лет, 23 % в возрасте 23–35 лет, 10 % в возрасте от 18 до 23 лет и 0 % в возрасте младше 18 лет. Наиболее предпочтительным механизмом защиты, выбранным каждой возрастной группой, является установка антивирусного обеспечения. Женщины предпочитают установку

антивирусного программного обеспечения в качестве защиты от вредоносных программ, тогда как мужчины отмечают как установку антивируса, так и скачивание пиратских копий в качестве меры успешной защиты. На установку антивируса больше всего полагаются студенты ПОО, настройку файервола предпочитают работающие опрошенные, отказ от скачивания пиратских копий импонирует студентам вузов.

При обсуждении рисков, связанных с использованием пиратской версии компьютерной игры, более 50 % опрошенных в возрасте менее 18 лет отметили хищение персональных данных и игровых аккаунтов, взлом персонального компьютера и кражу финансовой информации. Среди молодежи в возрасте 18–23 лет более 50 % отметили хищение персональных данных и взлом персонального компьютера. При этом разброс мнений опрошенных в возрасте старше 23 лет нигде не превышал 50 %, однако именно эта группа опрошенных выказала наибольшее затруднение при ответе на данный вопрос (39 % среди опрошенных в возрасте от 23 до 35 лет и 43 % в возрасте от 35 лет и старше). Среди женщин на первом месте стоят риски, связанные с хищением персональных данных (51 %), на втором – взлом персонального устройства через игру (39 %), а на третьем – хищение игрового аккаунта (38 %). Среди мужчин на первом месте стоят риски взлома персонального устройства через игру (70 %), на втором – удаленное управление устройством (49 %), а на третьем – хищение персональных данных и кража финансовой информации (по 47 %). Среди опрошенных любой занятости (как студенты, так и работающие) ключевыми рисками являются хищение персональных данных и взлом персонального устройства через игру.

Превалирующее большинство опрошенных отмечают, что нельзя делиться никакими персональными данными с другими людьми при использовании онлайн-игр. Однако некоторые опрошенные старше 18 лет готовы предоставить свой логин (18–23 года – 21 %, 23–35 лет – 29 %, старше 35 лет – 36 %). Следует отметить, что при этом 25 % подростков в возрасте младше 18 лет готовы предоставить другим пользователям как логин, так и пароль от своего аккаунта. Женщины и мужчины практически солидарны при ответе на данный вопрос: 68 % представителей обоих полов не желают делиться персональными данными, а 29 % женщин и 30 % мужчин готовы предоставить информацию лишь о логине. В категории «Занятость» мы наблюдаем примерно такую же картину: подавляющее большинство отказывается делиться персональной информацией и примерно треть пользователей готовы предоставить свой логин.

Половина пользователей (за исключением возрастной прослойки в возрасте 23–35 лет) отмечают, что компьютерные игры могут стать инструментом для социальной инженерии. Лишь 26 % опрошенных в возрасте 23–35 лет соглашаются с этим фактом. Достаточно большое количество опрошенных затруднились ответить на данный вопрос. Наибольшее количество затруднившихся – в возрасте до 18 лет (50 %), наименьшее количество затруднившихся – в возрасте старше 35 лет (21 %). Большее количество мужчин (51 %) считают, что это возможно, по сравнению с 44 % женщин. При этом большее количество женщин (37 %) затруднилось дать ответ на этот вопрос по сравнению с мужчинами (32 %). Половина студенческой молодежи уверена, что игры могут стать инструментом для социальной инженерии, тогда как лишь 37 % работающих опрошенных согласны с этим утверждением. При этом вторая половина студентов ПОО затрудняется ответить на данный вопрос, тогда как среди студентов вузов только 32 % затруднившихся, а среди работающих опрошенных – 37 %.

Наиболее категорично возражают против сбора биометрических данных посредством видеокамеры и микрофона опрошенные в возрасте 23–35 лет (39 %), выбравшие ответ «Полностью не согласен». В остальных возрастных категориях опрошенные были менее категоричны, но при этом скорее несогласны с данной процедурой (выбор ответа «Скорее несогласен, чем согласен» у 50 % опрошенных в возрасте младше 18 лет, 44 % опрошенных в возрасте 18–23 лет и 57 % опрошенных в возрасте старше 35 лет). Мужчины более категоричны при ответе на данный вопрос, чем женщины (43 % полностью несогласных мужчин против 25 % женщин), однако женщины тоже склоняются к несогласию с подобным сбором информации (46 % женщин скорее несогласны, чем согласны, по сравнению с 36 % мужчин). Больше половины студентов ПОО (56 %) категорически несогласны со сбором биометрических данных, тогда как студенты вузов и работающие менее категоричны и скорее несогласны, чем согласны (46 и 41 % соответственно).

Подавляющее большинство опрошенных не сталкивались с игроками, заставляющими передавать персональные данные или угрожающими в сети. При этом наибольший процент столкнувшихся с данной проблемой отмечается в возрасте младше 18 лет (25 %). Мужчины (11 %) чаще сталкивались с подобной ситуацией, чем женщины (7 %). Чаще всего с угрозами или требованиями предоставить персональные данные сталкиваются студенты ПОО (17 %) по сравнению со студентами вузов (7 %) и работающими опрошенными (7 %).

75 % опрошенных в возрасте младше 18 лет не хранят свои персональные данные на игровом устройстве. Напротив, 51 % опрошенных в возрасте старше 35 лет хранят свои персональные данные на устройстве, с которого играют в игры. Одна пятая всех опрошенных в возрасте старше 18 лет не задумывается об этом. Большее количество опрошенных мужчин (40 %) хранят свои персональные данные на игровом устройстве по сравнению с женщинами (37 %). При этом большее количество работающих опрошенных (46 %) хранят свои данные на игровом устройстве по сравнению со студентами вузов (36 %) и студентов ПОО (28 %).

Наибольшее количество опрошенных, противящихся использованию пиратских копий компьютерных игр, наблюдается среди тех, кому старше 35 лет (36 %). Наибольшее количество опрошенных, активно пользующихся пиратскими копиями, наблюдается в возрасте младше 18 лет (75 %). Женщины чаще пользуются пиратскими копиями, чем мужчины (64 % против 53 %). Большая часть опрошенных, пользующихся пиратскими играми, приходится на студентов ПОО (56 %) и студентов вузов (50 %), тогда как только 29 % работающих опрошенных прибегают к подобного рода продуктам.

Преобладающее большинство опрошенных всех возрастов не открывали незнакомые ссылки, полученные от незнакомых людей. Мужчины охотнее открывают незнакомые ссылки, чем женщины (13 % против 6 %). Студенты ПОО чаще открывают незнакомые ссылки (17 %), чем студенты вузов и работающие опрошенные (7 % в каждой группе).

Обсуждение

Подводя итоги аналитического обзора опроса, можно сделать ряд значимых выводов:

1. Опрошенные старше 35 лет, в целом, более небрежно относятся к вопросам, связанным с информационной безопасностью, чем студенческая молодежь: они нерегулярно обновляют антивирусное обеспечение, не владеют необходимой информацией по алгоритмам и способам защиты, хранят персональные данные на игровых устройствах и т. д.
2. В целом, мужчины более подготовлены в части защиты персональных данных и соблюдения режима информационной безопасности, чем женщины. Также студенческая молодежь тщательнее следует правилам информационной безопасности, чем работающие опрошенные.
3. При решении проблем, связанных с информационной безопасностью, студенческая молодежь, как правило, надеется на себя, в то

время как работающие опрошенные старшего возраста обращаются в техподдержку, т. е. привлекают сторонних специалистов.
4. Студенты ПОО являются наиболее доверчивой группой среди опрошенных: они составляют большинство тех, кто готов предоставлять свои персональные данные другим людям и переходить по незнакомым ссылкам, предоставленным незнакомыми игроками.
5. Большинство опрошенных всех возрастов и групп не понимают, что такое социальная инженерия и ее механизмы, соответственно потенциально уязвимы к данного рода нарушению информационной безопасности.
6. Большинство опрошенных всех возрастов и групп категорически не согласны с автоматическим сбором биометрических данных, воспринимая это как угрозу информационной безопасности.
7. Чем старше возрастная категория опрошенных, тем более законопослушными они являются, отказываясь пользоваться пиратским игровым контентом.

Полученные в ходе опроса данные и анализ результатов опроса позволяют скорректировать образовательные моменты, связанные с информационной безопасностью, и подготовить методические комплексы с учетом возрастных, гендерных и трудовых особенностей, направленные на предоставление знаний о способах и приемах защиты персональных данных, а также на противодействие мошенническим действиям при использовании видеоигр в качестве программного обеспечения.

Литература

1. *Житнюк П.* Киберугрозы реальные и выдуманные // Россия в глобальной политике. 2010. Т. 8. № 2. С. 186–196.
2. *Кухаркин А.В.* Киберугрозы и защита информации // Обозреватель. 2012. № 10(273). С. 94–104.
3. *Осипенко А.Л.* Киберугрозы в отношении несовершеннолетних и особенности противодействия им с применением информационных технологий // Общество и право. 2019. № 3(69). С. 23–31.
4. *Семеко Г.В.* Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. 2020. № 1. С. 77–96.

Информация об авторах

Николаева Милана Олеговна, магистр физико-математических наук, младший научный сотрудник сектора мониторинга и анализа деструктивных проявлений в образовательной среде Научно-исследовательского центра мониторинга и профилактики деструктивных проявлений в образовательной среде, Челябинский институт развития профессионального образования (ГБУ ДПО ЧИРПО), г. Челябинск, Российская Федерация, ORCID: https://orcid.org/0009-0003-7198-9995, e-mail: nikolaeva-15@bk.ru

Селютин Александр Анатольевич, кандидат филологических наук, заведующий сектором разработки программ социокультурной адаптации и интеграции иностранных студентов и детей-инофонов Научно-исследовательского центра мониторинга и профилактики деструктивных проявлений в образовательной среде, Челябинский институт развития профессионального образования (ГБУ ДПО ЧИРПО), доцент кафедры теоретического и прикладного языкознания историко-филологического факультета, Челябинский государственный университет (ФГБОУ ВО ЧелГУ), г. Челябинск, Российская Федерация, ORCID: https://orcid.org/0000-0002-0575-9521, e-mail: alexsell@mail.ru

Information Security while Using Video Games

Milana O. Nikolaeva
Chelyabinsk Institute of Vocational Education Development
Chelyabinsk, Russia
ORCID: https://orcid.org/0009-0003-7198-9995
e-mail: nikolaeva-15@bk.ru

Alexander A. Selutin
Chelyabinsk Institute of Vocational Education Development
Chelyabinsk, Russia
ORCID: https://orcid.org/0000-0002-0575-9521
e-mail: alexsell@mail.ru

The article is devoted to the information security during the game online-process. The foundation of the article includes the results of the online-survey with 156 participants. The analysis of the survey was performed using three categories: age, gender and occupation. The questions concerned topical issues on the agenda: the violation of information security mostly connected with the human factor. The analysis of responses was performed with the percentage correlation and determining the relative value. The authors draw the conclusion about the degree of readiness among respondents to the struggle against fraud actions in computer games as well as about the necessity to correct the educational components connected with skills and competences of information security. The researchers specifically mark the difference in perception of own safety in video games due to age, gender and occupation of the respondents, pointing at a high degree of caution among the respondents of older age and a greater carelessness among younger users of computer games. The results of the survey and conclusions drawn from the analysis may be used to form the complex of preventive actions aimed at the reduction of cybercriminal threats and risks of destructive behavior while communicating in the Internet space.

Keywords: computer game, information security, survey, algorithm, protection, personal data.

For citation: Nikolaeva M.O., Selutin A.A. Information Security while Using Video Games *// Digital Humanities and Technology in Education (DHTE 2023): Collection of Articles of the IV International Scientific and Practical Conference. November 16–17, 2023 /* V.V. Rubtsov, M.G. Sorokova, N.P. Radchikova (Eds). Moscow: Publishing house MSUPE, 2023. 513–523 p. (In Russ., abstr. in Engl.).

Information about the authors

Milana O. Nikolaeva, PhD in Psychology, Junior Research Associate, Scientific Research Center for Monitoring and Prevention, Chelyabinsk Institute

of Vocational Education Development, Chelyabinsk, Russia, ORCID: https://orcid.org/0009-0003-7198-9995, e-mail: nikolaeva-15@bk.ru

Alexander A. Selutin, PhD in Filology, Head of the Department, Scientific Research Center for Monitoring and Prevention, Chelyabinsk Institute of Vocational Education Development, Chelyabinsk, Russia, ORCID: https://orcid.org/0000-0002-0575-9521, e-mail: alexsell@mail.ru