Изучение вопросов социальной инженерии и организационно-правовых аспектов информационной безопасности раздела «Цифровая грамотность» курса информатики среднего общего образования с применением кейсов

The Study of Social Engineering and Organizational and Legal Aspects of Information Security in the Section "Digital Literacy" of the Course of Computer Science of Secondary General Education with the Use of Cases

Получено 22.09.2023 Одобрено 25.09.2023 Опубликовано 25.10.2023 УДК 37.01 DOI: 10.12737/1998-0744-2023-11-5-46-58

САМЫЛКИНА Н.Н.,
д-р пед. наук, доцент, профессор кафедры теории и методики обучения математике и информатике Института математики и информатики, ФГБОУ ВО «Московский педагогический государственный университет», г. Москва

e-mail: nsamylkina@yandex.ru

ДОРОХОВА А.А.,
магистрант 2 курса Института математики и информатики, ФГБОУ ВО «Московский педагогический государственный университет», г. Москва

e-mail: aa.dorokhova@mpgu.su

SAMYLKINA N.N.,
Doctor of Pedagogical Sciences, Associate Professor, Department of Theory and Methodology of Teaching Mathematics and Informatics, Institute of Mathematics and Informatics, Moscow Pedagogical State University, Moscow

e-mail: nsamylkina@yandex.ru

DOROKHOVA A.A.,
Master's Degree Student, Institute of Mathematics and Informatics, Moscow Pedagogical State University, Moscow

e-mail: aa.dorokhova@mpgu.su

Аннотация

Статья посвящена подготовке и использованию кейсов по социальной инженерии для рассмотрения организационно-правовых аспектов информационной безопасности. С ростом доступности цифровых инструментов тема информационной безопасности личности остается актуальной, поскольку доля обманутых мошенниками людей только увеличивается. Особенно стали популярными сложные фишинговые сценарии и атаки посредством социальных сетей и мессенджеров. Все более востребованным в общем образовании становится формирование целостного представления в области обеспечения информационной безопасности с упором на формирование цифровых компетенций в области информационной этики и права. Для достижения предметных результатов по данной теме учителям информатики предлагается использовать интерактивные кейсы по социальной инженерии в курсе информатики на уровне среднего общего образования.

Ключевые слова: информационная безопасность, социальная инженерия, фишинг, кибербуллинг, персональные данные, кейсы, информатика, защита информации, информационная этика, информационное право, правовые нормы.

Abstract

The article is devoted to the preparation and use of cases on social engineering to consider organizational and legal aspects of information security. With the increasing availability of digital tools, the topic of personal information security remains relevant, as the proportion of people who are deceived by fraudsters is only increasing. Sophisticated phishing scenarios and attacks on social networks and messengers have become especially popular. The formation of a holistic view in the field of information security with an emphasis on the formation of digital competencies in the field of information ethics and law is becoming increasingly demanded in general education. To achieve subject outcomes on the topic, computer science teachers are encouraged to use interactive social engineering cases in a computer science course at the secondary general education level.

Keywords: information security, social engineering, phishing, cyberbullying, personal data, cases, computer science, information protection, information ethics, information law, legal regulations.

Актуальность изучения вопросов информационной безопасности тематического раздела «Цифровая грамотность» на уровне среднего общего образования

В соответствии с Указом Президента России № 203 от 9 мая 2017 г. утверждена «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы» [10], в которой информационная безопасность определена как одно из основных направлений развития информационных и коммуникационных технологий в России. Положения по реализации стратегии пересекаются с программой «Цифровая экономика Российской Федерации» [7], т.е. обеспечивают основные инфраструктурные элементы цифровой экономики: информационную инфраструктуру, информационную безопасность, нормативно-правовое регулирование информационной сферы, образование и подготовку кадров.

5 декабря 2016 г. № 646 была утверждена «Доктрина информационной безопасности Российской Федерации» [4]. Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности. Новые глобальные вызовы и угрозы, которые препятствуют развитию цифровой экономики в России, должны браться в расчет и, более того, необходимо их предупреждать. К таким вызовам относятся «*проблема обеспечения прав человека в цифровом мире, в том числе при идентификации (соотнесении человека с его цифровым образом), сохранности цифровых данных пользователя, а также проблема обеспечения доверия граждан к цифровой среде*» [4].

Государственные программы, совершенствующие экономическую систему, являются ориентиром для изменения образовательных стандартов всех уровней образования. Именно поэтому вопросам информационной безопасности уделяется большое внимание в обновлённых ФГОС общего образования. На вопросы информационной безопасности сделан акцент в актуальном тематическом разделе курса информатики «Цифровая грамотность», где рассматриваются вопросы функционирования цифровых устройств и компьютерных сетей [2]. Позиционирование вопросов информационной безопасности в обязательном разделе «Цифровая грамотность» в начале изучения курса информатики значительно повышает значимость этих вопросов, а также позволяет изучать в интегративном режиме вопросы информационной безопасности и функционирования цифровых устройств. Уровень среднего общего образования является образовательным полигоном пробной деятельности для успешного профессионального самоопределения учащихся, поскольку именно на этом уровне реализуются программы предпрофессиональной подготовки школьников (инженерные и информационно-технологические классы). На этом уровне образования обучающиеся уже готовы рассматривать правовые документы. При этом следует понимать, что тематический раздел «Цифровая грамотность» является обязательным для всех профилей обучения, соответственно во всех классах предпрофессионального обучения, и его содержательное наполнение и требования к результатам освоения программы не различаются на базовом и углубленном уровнях изучения информатики в среднем общем образовании. По предлагаемым примерным рабочим программам по информатике базового и углубленного уровней изучения содержание вопросов информационной безопасности разнесено по разным классам и скорректировано по объему отведенного времени. На базовом уровне изучения информатики выделена тема «Основы социальной информатики» в 11 классе в объеме 3 ч. На углубленном уровне изучения информатики в 10 классе тема называется «Информационная безопасность» в объеме 7 ч [8; 9].

Основные понятия темы и их взаимосвязь

Раскрывая вопросы использования различных «средств защиты информации в компьютерах, компьютерных сетях и автоматизированных информационных системах» [2], мы пользуемся уже устоявшимися понятиями,

такими как информационная безопасность, защита информации, информационная этика, информационное право, правовые (законодательные) нормы. В начале изучения целесообразно разделить понятия «информационная безопасность» и «защита информации», они не синонимичны. Понятие «информационная безопасность» следует рассматривать достаточно широко, как *весь комплекс мер по обеспечению защиты информации в информационных системах* [6].

В соответствии со ст.16 Федерального закона «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ «*Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:*

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации» [11].

Поскольку все эти нормы установлены в законодательстве нашей страны, они считаются правовыми нормами и относятся к сфере информационного права.

Информационное право – *комплексная отрасль права, регулирующая общественные отношения, связанные с созданием, хранением, обработкой, распространением, использованием информационных ресурсов; развитием и использованием новых технологий работы с информацией и технологий её передачи в системах и сетях коммуникаций; обеспечением информационной безопасности общества, государства и человека*. [1].

Как правило, законодательство в информационной сфере (информационное право) всегда несколько запаздывает и узаконивает уже сформировавшиеся отношения, которые длительный период времени определялись этическими нормами в информационной сфере [6].

Информационная этика *может быть определена как область этики, которая рассматривает принципы использования средств ИКТ и поведения в глобальной сети Интернет, вопросы использования и злоупотребления информацией, информационными системами для принятия каких-либо личных или профессиональных решений* [1].

Использование компьютерных систем во всех сферах современной жизни помимо преимуществ повлекло за собой появление большого ряда специфических проблем. Одной из таких проблем является необходимость обеспечения эффективной защиты информации, которая обусловлена ростом правонарушений, связанных с кражами и неправомерным доступом к данным посредством нарушения этических норм. Множество способов, психологических и социальных приёмов, методов и технологий, применяемых компьютерными злоумышленниками, которые позволяют получить конфиденциальную информацию, называется *социальная инженерия.*

Понятие «социальная инженерия» достаточно новое и пока не входит в число обязательных для рассмотрения школьниками. Но это понятие можно считать вспомогательным для объяснения сути явлений, происходящих в области информационной безопасности. Схематично взаимосвязь используемых понятий можно представить следующим образом (см. рис. 1 на с. 49).

Социальная инженерия – это метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Данное понятие используется в контексте устоявшихся терминов, которые находятся в определенном соотношении друг с другом. Социальная инженерия занимается тем, что с помощью воздействия на личность, происходит нарушение этических норм в информационной сфере. Это приводит к тому, что нарушается информационное право, и как следствие, возникает угроза информационной безопасности. Возникают проблемы в защите интересов личности и организаций. После обсуждения основных понятий по теме с опорой на нормативные правовые документы далее целесообразно разобрать проблемные ситуации и способы их разрешения, которые наиболее актуальны в текущий период времени, также используя правовую базу. Именно для этих целей был разработан специальный электронный ресурс в виде кейсов, который расположен

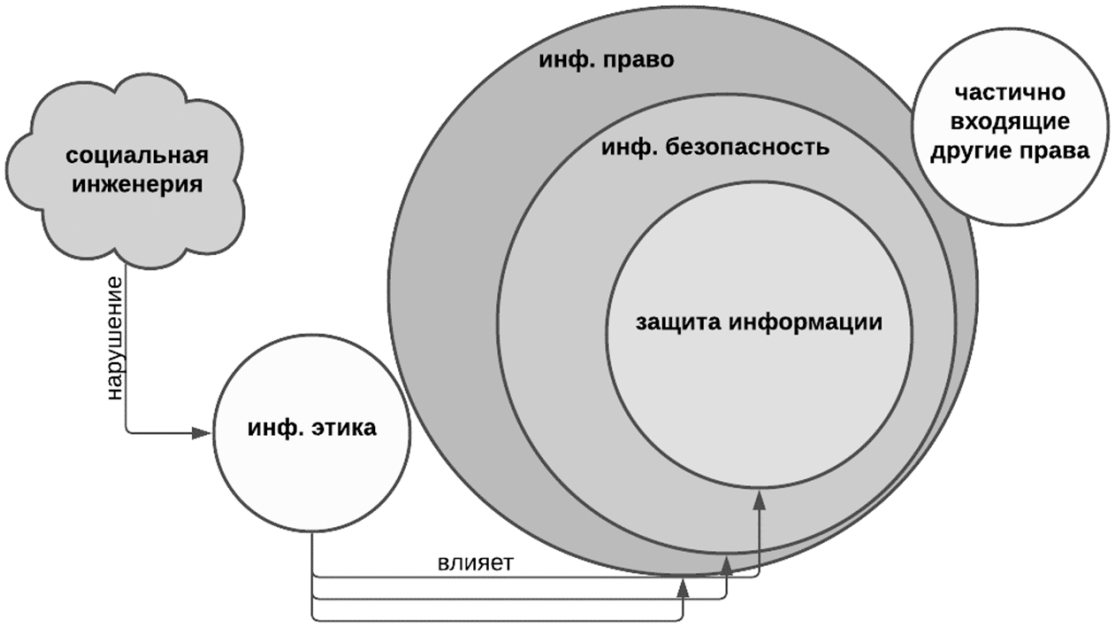

Рис. 1. Взаимосвязь основных понятий

на сайте: https://case.kocheshkoff.ru/ и может быть использован на уроках информатики.

Подготовка и использование кейсов по социальной инженерии

Для формирования практических навыков по теме был выбран активный метод обучения – **кейс-технология.** Кейс-технология дает возможность обучающимся проявить инициативу, активность и самостоятельность в согласовании с мнениями одноклассников, а также оставляет право каждого на собственное мнение. Более того, современные кейсы – это интерактивные цифровые ресурсы, которые несложно создать учителю по собственному сценарию.

Для создания интерактивных кейсов использовалось программное обеспечение iSpring Suite, зарегистрированное в едином реестре российских программ для электронных вычислительных машин и баз данных [5]. Был использован формат диалогового тренажера, который позволяет предусмотреть различные исходы событий благодаря созданию нескольких ветвей диалога в зависимости от выбранного варианта ответа. Кроме создания диалоговых тренажеров данный конструктор можно использовать и при создании тестов, опросов, курсов, видеолекций на основе PowerPoint. Программа iSpring Suite содержит встроенную библиотеку контента, из которой можно выбрать персонажа для диалогового тренажера и сцену. Также в этой программе можно загрузить озвучку для реплик героев.

Такой формат работы со старшеклассниками позволит реализовать предметные требования к результатам освоения основной образовательной программы среднего общего образования по данной теме:

– умение критически оценивать информацию, полученную из сети Интернет;

– понимание угроз информационной безопасности, использование методов и средств противодействия этим угрозам, соблюдение мер безопасности, предотвращающих незаконное распространение персональных данных [8; 9].

Рассмотрим подробнее процесс разработки цифровых кейсов. Первым шагом было непосредственное *написание сценария*. Была выбрана тематика каждого кейса, действующие лица, проработаны основной ход диалога и реплики героев. Вторым шагом были добавлены дополнительные варианты ответа и подготовлена схема ветвления сюжета для последующего перенесения в программу. Третьим шагом было создание диалогового тренажера на основе подготовленной схемы.

Четвертым шагом были озвучены персонажи. На пятом шаге была произведена окончательная проверка работы диалогового тренажера и выполнен экспорт в формате веб-сайта. Было разработано семь кейсов: пять в формате диалогового тренажера и два в формате «ситуация и вопросы по ней».

1. Кейс «Разочарование для шопоголика».
2. Кейс «Продолжай в том же духе!».
3. Кейс «Фейковый трейдинг».
4. Кейс «Такой обманчивый 900».
5. Кейс «Компьютерный мастер».
6. Кейс «Стикеры взамен на паспорт» (вопрос-ответ).
7. Кейс «Модель на любой товар» (вопрос-ответ).

В данной статье мы приводим содержание пяти кейсов. В случае отсутствия возможности использовать компьютеры с выходом в интернет можно воспользоваться бумажным вариантом кейса и провести деловую игру (тренинг по ролям). Рассмотрим каждый из кейсов более подробно. Схема ветвления сюжета приводится только для первого кейса.

Кейс «Разочарование для шопоголика»

1. **Предисловие.** Представьте себе, что Вы – успешный юрист, дающий консультации в сфере информационной безопасности, и прямо сейчас Вам поступил очередной звонок.

2. **Девушка.** Здравствуйте! Прошу, пожалуйста, помогите мне! Я совершенно не знаю, что мне делать!

3. **Юрист.** Здравствуйте! Давайте попробуем разобраться с вашей проблемой. Расскажите подробнее, что произошло.

4. **Девушка.** Понимаете, дело в том, что я давно хотела обновить свой гардероб. Сейчас из-за больших трат в связи с подготовкой к новогодним праздникам я отложила этот вопрос, но я не могла упустить возможность закупиться новыми вещами, ведь не поверите, мне на электронную почту пришло письмо от моего любимого сайта – Ламода, что сейчас действует акция: «При покупке 3-х вещей скидка 25%», и, конечно же, я не могла упустить такой шанс. Я долго выбирала и в итоге заказала себе пару кофточек и платье. Когда я все оплатила, с моей карты сняли больше требуемой суммы. Значительно больше! Я в недоумении! Кроме того, мне не пришло никакого подтверждения заказа, как это было всегда! Подскажите, что мне делать?!

5. **Юрист.** Какую сумму списали с Вашей карты?

6. **Юрист.** Вы сказали, что письмо пришло на электронную почту. Проверьте пожалуйста адрес отправителя, от кого пришло письмо, и продиктуйте его?

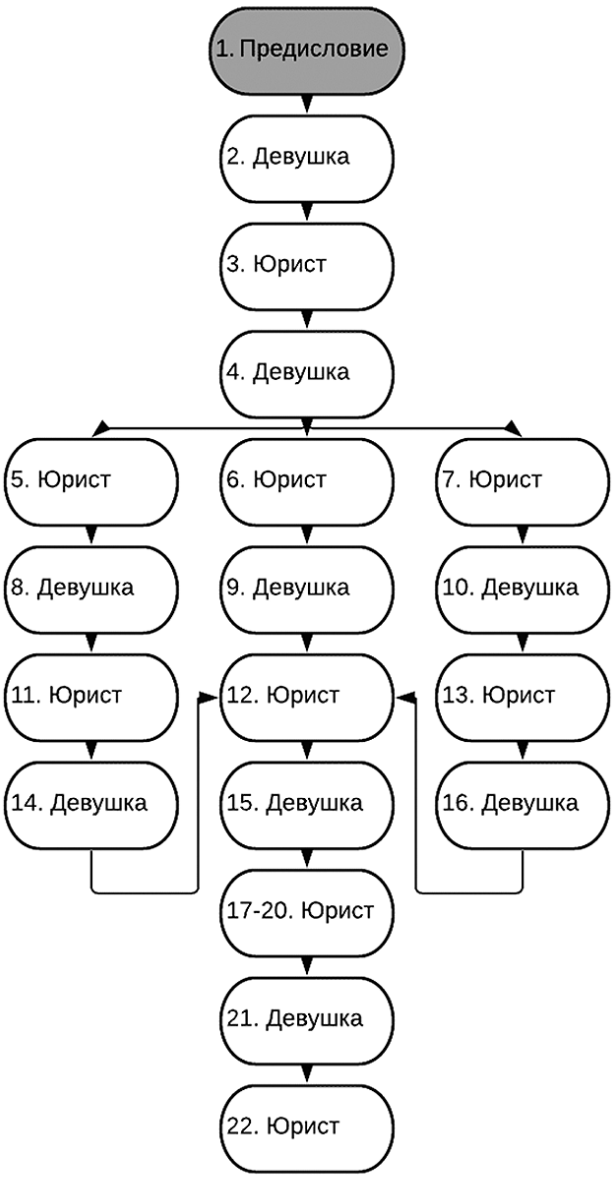

Рис. 2 Схема кейса «Разочарование для шопоголика»

7. **Юрист.** Вы сказали, что это Ваш любимый магазин. Часто ли Вы делаете там покупки?

8. **Девушка.** С карты списали 20 тысяч, хотя заказ при этом был примерно на 12 тысяч.

9. **Девушка.** sale@larnoda.ru Хмм, кажется, в адресе сайта ошибка – написано Ларнода, а не Ламода, но в первый раз я этого не заметила.

10. **Девушка.** Да, я пользуюсь этим магазином уже больше двух лет. Последний раз я заказывала вещи 3 месяца назад.

11. **Юрист.** Возможно, это ошибка сайта либо банковской системы. Попробуйте на сайте найти раздел «контакты» и свяжитесь с представителем магазина для уточнения деталей произошедшего.

12. **Юрист.** Проверьте, пожалуйста, внимательно, при переходе по ссылке из письма, какой адрес сайта отображается в адресной строке?

13. **Юрист.** Я думаю, что Вам и ранее приходили письма с рассылкой от этого магазина. Сравните, пожалуйста, адреса отправителей последнего письма и полученных ранее, например, несколько месяцев назад.

14. **Девушка.** Вы знаете, я не могу найти на сайте раздел с контактами, хотя уже все просмотрела, но я точно помню, что раньше он был.

15. **Девушка.** Так, я вижу адрес lannoda.ru Как такое могло произойти?

16. **Девушка.** Да, я нашла письмо полугодовой давности, адреса действительно различаются. В последнем письме адрес sale@larnoda.ru, а в раннем письме адрес sale@lamoda.ru.

17. **Юрист.** Скорее всего, Вы попали на фишинговую рассылку и произвели оплату на фишинговом сайте. Это значит, что данные Вашей карты попали в руки злоумышленников. В самые кратчайшие сроки позвоните в банк и заблокируйте карту, с которой была произведена оплата.

18. **Юрист.** К сожалению, Вы не единственный человек, кто столкнулся с такой проблемой. Фишинговые рассылки и сайты сейчас очень распространены. Этим методом социальной инженерии активно пользуется большое количество мошенников.

19. **Юрист.** Вы можете обратиться к нотариусу за нотариальным обеспечением доказательств существования этого сайта в интернете. Также не лишним будет самостоятельно сделать скриншоты страниц этого сайта, включая страницу контактов, если она имеется. Если мошенник известен, то можно подать исковое заявление о взыскании неосновательного обогащения в зависимости от суммы в мировой или районный суд (ГК РФ ст. 11.02) [3].

20. **Юрист.** Впредь будьте внимательны: при получении подобных рассылок в СМС, на электронную почту, социальные сети, мессенджеры обращайте внимание на адрес отправителя, его имя, прикрепленные к письму ссылки и документы, грамматические, орфографические и дизайнерские ошибки на сайтах, наличие страницы контактов, отсутствие пользовательских соглашений, проверьте, что подключение к сайту защищено – используется протокол соединения https:// (указывается в начале адресной строки). Все эти признаки могут свидетельствовать о том, что сайт является фишинговым, и создан мошенниками для получения Ваших личных данных, в том числе платежных (данных банковских карт и счетов).

21. **Девушка.** Спасибо большое за подробную консультацию! Теперь я буду внимательнее и сейчас же заблокирую карту и обращусь к нотариусу. До свидания!

22. **Юрист.** До свидания!

Для сценария кейса, представленного выше, на рисунке 2 изображена схема ветвления сюжета.

Данный кейс направлен на формирование понятий фишинговый сайт, фишинговая ссылка, а также на формирование умения выявлять их с учетом изложенных в кейсе признаков.

При работе с диалоговым тренажером можно предложить обучающимся самостоятельно сформулировать определения, рассматриваемые в кейсе, признаки фишингового сайта и записать их в тетрадь. Также предложить свои способы выявления фишинга. При обсуждении предложенной ситуации можно рассмотреть другие способы получения от мошенника фишинговой ссылки и способы защиты, обсудить с обучающимися, попадали ли они в схожие ситуации.

Кейс «Продолжай в том же духе!»

1. **Предисловие.** Вам пишет Ваш друг, который живет в другом городе, и Вы с ним регулярно общаетесь в интернете.

2. **Друг.** Привет. Ты же знаешь, что я давно интересуюсь историей XX века, знаю много непопулярных и интересных фактов. Недавно я решил создать свой YouTube-канал и поделиться этой информацией с такими же увлекающимися историей людьми. Я уже выложил несколько видео на канал. Кстати, попозже скину ссылку – подпишись и посмотри, надеюсь, тебе понравится. В целом дела идут хорошо – у меня уже около 1000 подписчиков, я думаю, что за месяц это отличный результат! Но, не все идет так гладко, как хотелось бы…

3. **Вы.** Привет! Отлично, я давно тебе говорил, что тебе нужно поделиться своими находками с другими! Круто, что ты решил этим всерьез заняться. 1000 подписчиков - отличное начало, думаю дальше будет еще больше. Ты сказал, что все не так гладко – что случилось?

4. **Друг.** В последнее время я заметил, что под каждым видео начали появляться комментарии от одного человека – он постоянно оскорбляет меня. Есть люди, которые пишут конструктивную критику, я им отвечаю, и в ходе дискуссии рождается истина. Но этот человек пишет абсолютно необоснованную ерунду.

5. **Вы.** А что именно он пишет?

6. **Друг.** Последний его комментарий был таким: «Голос – жуть, слушать невозможно! Все отписывайтесь, если не хотите быть как он!».

7. **Вы.** А что еще он тебе писал?

8. **Вы.** А ты не пробовал его заблокировать?

9. **Вы.** А что ты ему на это ответил?

10. **Друг.** Да много всего. Писал, что я зануда и, вообще, чтобы больше ничего никогда не снимал.

11. **Друг.** Пробовал, он создал еще один аккаунт.

12. **Друг.** Пока я ничего ему не отвечал, даже не хочется вступать с ним в спор.

13. **Вы.** Действительно, очень глупые и необоснованные комментарии. Просто заблокируй его.

14. **Вы.** Я считаю, что тебе нужно ответить ему. Напиши, что раз ему не нравится – пусть просто не смотрит твои видео.

15. **Вы.** Это похоже на кибербуллинг. Правильно, не нужно реагировать на эту агрессию в твою сторону, это лишь заставит его писать подобные комментарии все чаще и чаще.

16. **Вы.** Какой настойчивый человек, это напоминает кибербуллинг. Думаю, тебе не нужно отвечать на его комментарии, просто продолжай блокировать все его новые аккаунты, и со временем ему это просто надоест, и он оставит тебя в покое.

17. **Друг.** Думаю, ты прав. Так и поступлю.

18. **Друг.** Не думаю, что это правильно. Это похоже на кибербуллинг, и если я буду отвечать на каждый такой его комментарий, то это лишь заставит писать его все чаще и чаще.

19. **Вы.** Кроме того, я посмотрел твои видео, это действительно очень интересно! Продолжай в том же духе. Людям это нравится, ведь на 1000 подписчиков, действительно заинтересованных твоим контентом, нашелся всего один такой завистник. Ты молодец!

20. **Вы.** Да, ты прав, я не подумал об этом. Думаю, тебе и вправду не нужно отвечать на его комментарии, просто продолжай блокировать все его новые аккаунты, и со временем ему это просто надоест, и он оставит тебя в покое.

21. **Друг.** Спасибо тебе огромное за поддержку, а то я уже начал переживать из-за него. Но теперь я понял, что мои видео действительно полезные и интересные и я буду продолжать заниматься своим любимым делом.

Для сценария кейса, представленного выше, на рисунке 2.2 изображена схема ветвления сюжета.

Данный кейс направлен на формирование понятия кибербуллинг, а также на формирование умения вести себя в схожей ситуации. Его можно использовать в основной школе, где он впервые используется.

Несмотря на то, что обучающиеся должны знакомиться с этим термином еще в основной школе, мы вновь возвращаемся к этому понятию в старшей школе. Это связано с тем, что школьники должны знать и уметь правильно себя вести при столкновении с ки-

бербуллером, которых сейчас в интернете огромное количество. Кроме того, если ситуация не ограничивается разовыми оскорблениями, а перерастает в угрозы, преследование, то в старшей школе точно стоит говорить о правовой составляющей вопроса.

При работе с диалоговым тренажером следует обсудить само понятие кибербуллинг: что оно в себя включает, выработать правильную модель поведения при столкновении с обидчиком. Можно осуществить самостоятельный поиск информации о мерах наказания в нормативно-правовых актах, регулирующих различные аспекты понятия кибербуллинг. Также стоит обсудить с обучающимися их личный опыт – сталкивались ли они с кибербуллингом в свой адрес или адрес своих знакомых.

Кейс «Продолжай в том же духе!» может быть рассмотрен в курсе информатики основного общего образования при изучении такой темы, как сетевой этикет, при работе с электронной почтой, общении на форумах, в чатах.

Кейс «Фейковый трейдинг»

1. **Предисловие.** Вы уже больше месяца играете в онлайн-игру с человеком, с которым познакомились в этой же игре. Во время очередного матча у вас состоялся следующий диалог.

2. **Он.** Видел, какой я себе инвентарь собрал?

3. **Вы.** Да, классно. Наверное, дорого стоит?

4. **Он.** Да, почти 30 тысяч все вместе стоит.

5. **Вы.** Откуда у тебя такие деньги?

6. **Он.** У меня есть друг, который уже много лет занимается обменом вещей. Выгодно обменивает несколько дешевых на дорогие. Он мне и помог.

7. **Вы.** Ого, классно! А он может и мне так сделать?

8. **Он.** Обычно, он этим за деньги занимается, но я могу у него спросить.

9. **Вы.** Было бы здорово.

10. **Он.** Я ему написал, он согласен, но ему будут нужны логин и пароль от твоего аккаунта.

11. **Вы.** А сколько это займет времени?

12. **Вы.** Окей, вот логин и пароль – grandmaster, 1is2tsvT@%sgd.

13. **Вы.** А ты тоже ему давал свой логин и пароль?

14. **Он.** По-разному, зависит от того, есть ли предложения на обмен или нет.

15. **Он.** Хорошо, я ему отправил данные, жди.

16. **Он.** Да, конечно, у него они до сих пор есть. Как только появляются выгодные предложения – он заходит и обменивает вещи.

17. **Он.** *прошло несколько часов*. Всё, все твои вещи мы вывели и продали, а на аккаунте играли с читами, и теперь он будет заблокирован. Спасибо за доверие, но больше не попадайся на такой развод. *Вы добавлены в черный список и больше не можете отправлять сообщения пользователю*

18. **Вы.** Знаешь, я так подумал, что это выглядит странно. Я бы мог и сам обменять вещи. Он может рассказать, как он это делает и на какой площадке?

19. **Он.** Нет, ему это не выгодно. Вдруг ты пойдешь всем остальным рассказывать?

20. **Вы.** Нет, я никому не буду про это рассказывать, обещаю.

21. **Он.** Окей, если тебе не нужен нормальный инвентарь, то так и сиди со своим старым. *Вы добавлены в черный список и больше не можете отправлять сообщения пользователю*

22. **Вы.** Видимо, он пытался развести меня на вещи или я вообще мог бы остаться без своего аккаунта. Хорошо, что я не отправил ему логин и пароль. Надо быть внимательнее и осторожнее при знакомстве с людьми в интернете, даже если Вы с ними общаетесь достаточно долго.

Данный кейс направлен на формирование умения обращаться со своими персональными данными.

При работе с диалоговым тренажером можно предложить обучающимся перечислить, какие данные относятся к персональным, какие нормативно-правовые акты регулируют работу с персональными данными и их защиту, какая ответственность наступает в случае их разглашения третьими лицами. Кроме того, можно обсудить, где используются персональные данные человека и возможно ли их разглашение не по вине их собственника.

Кейс «Фейковый трейдинг» может быть интегрирован с темой «Информационные

системы». На его примере может быть рассмотрена организация информационной системы, механизм ее работы и уровни защиты и непосредственно базы данных, в которых могут храниться персональные данные пользователя.

Кейс
«Такой обманчивый 900»

1. **Предисловие.** Вам поступает телефонный звонок с короткого номера 900, Вы отвечаете на него, понимая, что это номер банка.

2. **Вы.** Алло, здравствуйте!

3. **Банк.** Добрый день, меня зовут Наталья, я являюсь сотрудником службы безопасности Сбербанка. Михаил Юрьевич, с Вашей карты совершен подозрительный перевод Прокофьевой Елизавете Сергеевне на сумму 4300 рублей. Вы совершали этот перевод?

4. **Вы.** Нет.

5. **Банк.** Михаил Юрьевич, у Вас карта используется в основном в Москве, Вы не входили в Сбербанк Онлайн из Саратова?

6. **Вы.** Нет.

7. **Банк.** Михаил Юрьевич, что мне делать с этой операцией: подтверждать или отклонять?

8. **Вы.** Отклонять.

9. **Банк.** Для отмены операции нужно Вас идентифицировать. Идентифицировать можно по номеру договора, личному коду id или по номеру действующей карты. Как Вы будете проходить идентификацию?

10. **Вы.** По номеру карты.

11. **Банк.** Михаил Юрьевич, номер карты необходимо по одной цифре назвать автоматизированной системе ввода данных. Сейчас я Вас на нее переключу. Готовы?

12. **Вы.** Да, готов.

13. **Робот.** Автоматизированная система ввода данных Сбербанк, назовите код после звукового сигнала. *Звуковой сигнал*

14. **Вы.** *Назвать номер своей карты*

15. **Вы.** *Положить трубку*

16. **Банк.** Робот проверил правильность ввода. Сейчас на Ваш телефон придет СМС с официального номера 900. Там будет код, который нужно сообщить роботу. Это код отмены операции.

17. **Вы.** Да, код пришел.

18. **Банк.** Вы готовы его произнести? Перевожу на робота.

19. **Вы.** *Произнести код*

20. **Банк.** Спасибо, операция отменена! *Повесили трубку*

21. **Вы.** *На телефон приходит СМС-уведомление о списании с карты 10.000 рублей. Вы решаете позвонить в банк*

22. **Сотрудник.** Добрый день, меня зовут Никита, чем я могу Вам помочь?

23. **Вы.** Добрый день, мне сейчас звонили из банка, сказали, что произведен подозрительный перевод, для отмены попросили назвать номер карты и код из СМС. После этого пришло СМС-уведомление, что с карты списали 10 тысяч рублей.

24. **Сотрудник.** Очень сожалею, но Вам звонили мошенники. Я не могу отменить перевод денежных средств, так как он уже совершен. В данной ситуации Вы можете обратиться с заявлением в полицию. Чтобы таких ситуаций больше не происходило, могу предложить Вам установить суточный лимит на денежные переводы. Он позволяет в течение дня переводить не более установленной суммы, отсчет суток начинается с первого перевода. Для перевода сверх установленного лимита Вам будет необходимо обратиться лично в банк.

25. **Вы.** Хорошо, спасибо большое.

26. **Сотрудник.** Всего доброго, до свидания!

27. **Вы.** *Позвонить в банк для уточнения информации*

28. **Вы.** *Продолжить заниматься своими делами*

29. **Сотрудник.** Добрый день, меня зовут Никита, чем я могу Вам помочь?

30. **Вы.** Добрый день, мне сейчас звонили из банка, с номера 900, сказали, что произведен подозрительный перевод, для отмены попросили назвать номер карты и код из СМС. Я положил трубку и хочу узнать, все ли в порядке с моей картой?

31. **Сотрудник.** Одну минуту, проверяю информацию. Да, с Вашей картой все в порядке, Вам звонили мошенники. Вы правильно сделали, что положили трубку. Если подобные ситуации повторятся, никогда никому не сообщайте данные своей карты и коды из СМС-уведомлений, с помощью этих данных мошенники могут списать средства с Вашей

карты. Кроме того, могу предложить Вам установить суточный лимит на денежные переводы. Он позволяет в течение дня переводить не более установленной суммы, отсчет суток начинается с первого перевода. Для перевода сверх установленного лимита Вам будет необходимо обратиться лично в банк.

32. **Вывод.** Вам звонили мошенники. Вы правильно сделали, что положили трубку. Если подобные ситуации повторятся, никогда никому не сообщайте данные своей карты и коды из СМС-уведомлений, с помощью этих данных мошенники могут списать средства с Вашей карты. Кроме того, Вы можете установить суточный лимит на денежные переводы. Он позволяет в течение дня переводить не более установленной суммы, отсчет суток начинается с первого перевода. Для перевода сверх установленного лимита Вам будет необходимо обратиться лично в банк. Если же Вы сообщили данные карты мошенникам, в ближайшее время позвоните сотрудникам банка для блокировки карты и обратитесь в полицию.

Данный кейс также направлен на формирование умения обращаться со своими персональными данными.

К числу самых популярных целей мошенников относится получение доступа к денежным средствам жертвы путем компрометации секретных данных банковской карты, в частности CVV/CVV2 кода. Предложенная ситуация описывает именно эту схему злоумышленников, которая до сих пор является актуальной и широко применяемой.

При работе с диалоговым тренажером можно предложить обучающимся обсудить произошедшую ситуацию с точки зрения жертвы и с точки зрения мошенника, подробно обговорить уязвимые места банковской системы, правила хранения данных банковской карты, совершения платежей в интернете, общения с незнакомыми или малознакомыми людьми на тему ваших денежных средств. Отдельно можно обсудить технические возможности совершения мошеннических телефонных звонков с официальных номеров банка и способы их распознавания. Стоит упомянуть о том, что сотрудники банка никогда не будут запрашивать у вас секретные данные карты и коды подтверждения из СМС или пуш-уведомлений.

Кейс «Такой обманчивый 900» лучше рассматривать непосредственно при изучении различных аспектов информационной безопасности. Также он может быть использован на уроках финансовой грамотности, что позволяет достичь определенных метапредметных результатов.

Кейс «Компьютерный мастер»

1. **Предисловие.** Несколько лет назад Вы помогли другу собрать новый компьютер, но через некоторое время Вы переехали в другой город. Связь с другом Вы поддерживаете в социальных сетях. Однажды Вы получили от него следующее сообщение.

2. **Друг.** Привет. Не хотел тебя беспокоить по этому вопросу, но с моим компьютером происходит что-то странное. Некоторое время назад он начал тормозить, и так как я не очень в этом всем разбираюсь, я вызвал компьютерного мастера, чтобы он посмотрел, что происходит. Его номер я нашел на объявлении в своем подъезде.

3. **Друг.** Первое время все было хорошо. Мастер сказал, что он почистил компьютер от ненужных системных файлов, обновил драйвера. Но он предупредил, что через некоторое время могут снова начаться проблемы, потому что установлено всего 4 ГБ оперативной памяти и этого мало. Сказал, что может обновить и добавить еще, если понадобится.

4. **Вы.** Привет! Да, помню, когда собирал, 4 ГБ еще было достаточно для работы и для игр. И что сейчас в итоге получилось?

5. **Друг.** Как и сказал мастер, компьютер стал снова тормозить, я ему позвонил, он приехал и сказал, что добавил оперативной памяти до 8 ГБ. Этого будет достаточно? Потому что особого прироста быстродействия я не вижу.

6. **Вы.** Нужно посмотреть, какую конкретно он поставил оперативную память, на какой частоте она работает и работает ли в двухканальном режиме. Зайди в настройки системы и отправь мне скриншот.

7. **Друг.** *Присылает скриншот*

8. **Вы.** Мда… У тебя здесь так и стоит до сих пор 4 ГБ оперативной памяти, причем

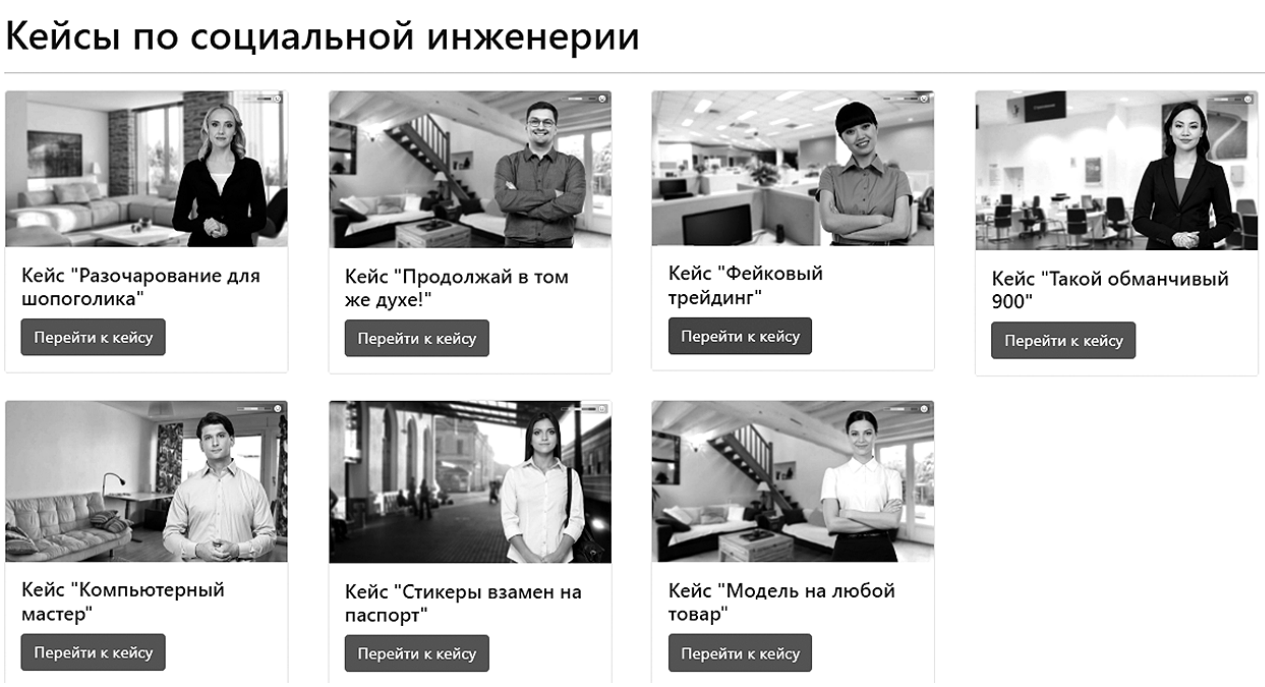

Рис. 3. Сайт с кейсами по социальной инженерии

видимо той же самой, которую я ставил при сборке. Скорее всего, мастер поставил программу-замедлитель, которая с каждым днем все больше и больше тормозила компьютер, чтобы потом взять еще с тебя денег якобы за установку дополнительной оперативной памяти.

9. **Друг.** И что теперь делать?

10. **Вы.** У тебя остался его номер?

11. **Вы.** Он оставил тебе акт выполненных работ?

12. **Друг.** Да, номер остался. Позвонить ему?

13. **Друг.** Да, он оставил мне какой-то акт.

14. **Вы.** Да, позвони ему, попробуй узнать, что он конкретно делал в последний раз.

15. **Вы.** Посмотри, есть ли в акте выполненных работ строка про замену оперативной памяти.

16. **Друг.** Он заблокировал мой номер, не могу ему дозвониться.

17. **Друг.** Да, здесь есть строка про установку 8 ГБ оперативной памяти.

18. **Вы.** Скорее всего, тебе попался мошенник. Я читал, что это одна из техник обратной социальной инженерии, которую применяют недобросовестные компьютерные мастера. Они заставляют жертву снова и снова обращаться к ним за помощью, при этом сами закладывают проблемы и неисправности в твой компьютер.

19. **Друг.** И что мне теперь делать?

20. **Вы.** Я бы посоветовал тебе обратиться в суд, если сумма, которую ты отдал за выполнение работ, достаточно большая для тебя. По закону «О защите прав потребителей» можно потребовать полного возмещения убытков либо устранения выявленных недостатков.

21. **Друг.** Эх, ладно… Спасибо за помощь. Пойду и попробую разобраться с этим. В следующий раз лучше проконсультируюсь с тобой.

22. **Вы.** Впредь будь внимательнее, обращайся в проверенный сервис, а не к частному мастеру. Жаль, что так вышло. Если что – пиши, всегда рад помочь.

Данный кейс направлен на формирование понятия обратной социальной инженерии.

При работе с диалоговым тренажером в основной школе в теме «Устройство компьютера» можно предложить рассмотреть различные варианты замены других комплектующих и их влияние на работу компьютера. В старшей школе можно подробнее разобрать вопросы установки программного обеспечения, которое замедляет работу компьютера, его сокрытие от пользователя, принцип работы, а также обсудить правовую сторону вопроса некаче-

ственного оказания услуг мастером и последствия, которые за это наступают.

Отдельно стоит упомянуть о том, что при озвучивании диалога специально были записаны только реплики собеседников, что позволяет достигнуть большего погружения в ситуацию. Комментировать правовые источники должен учитель или ведущий.

Для размещения кейсов был создан сайт https://case.kocheshkoff.ru/, который позволяет организовать удобный доступ к ним (рис. 3).

Следует отметить, что сценарии предложенных кейсов узнаваемы, поскольку основаны на актуальных и широко применяющихся мошеннических схемах, подобраны в соответствие с рассматриваемой возрастной группой. При использовании диалогового тренажера можно полноценно погрузиться в предложенную ситуацию и попробовать себя в роли эксперта, а также сформировать у обучающихся навык поведения в конкретной жизненной ситуации. Предложенные в статье кейсы прошли апробацию в школе и стали объектом интереса обучающихся не только с практической и содержательной точки зрения, но и как новый инструмент для представления собственного контента для различных мероприятий, например, защиты проектов.

Список литературы

1. *Босова Л.Л., Самылкина Н.Н.* Вопросы информационной этики и права в общеобразовательном курсе информатики. Материалы IX Международной научно-методической конференции посвященной 75-летию профессора Е.Ы. Бидайбекова и 35-летию школьной информатики: Математическое моделирование и информационные технологии в образовании и науке. – КазНПУ имени Абая, 2020.
2. *Босова Л.Л.* О новых подходах к изучению школьной информатики в условиях цифровой трансформации общества // Информатика в школе. 2022 г. №4(177) – с. 3.
3. Гражданский кодекс Российской Федерации от 30 ноября 1994 г №51-ФЗ https://www.consultant.ru/document/cons_doc_LAW_5142/
4. Доктрина информационной безопасности Российской Федерации». Утверждена 5 декабря 2016 г. № 646. https://www.consultant.ru/document/cons_doc_LAW_208191/
5. Единый реестр российских программ для электронных вычислительных машин и баз данных. https://www.ispring.ru/software-registry/
6. *Калинин И. А., Самылкина Н.Н.* Информатика. Углубленный уровень. 11 класс. М.: БИНОМ. Лаборатория знаний, 2013. 216 с.
7. Национальная программа «Цифровая экономика Российской Федерации». http://government.ru/info/35568/
8. Примерная рабочая программа среднего общего образования предмета «Информатика» (базовый уровень). Одобрена решением федеральных

References

1. Bosova L.L., Samylkina N.N. Issues of information ethics and law in the general education course of computer science. Materials of the IX International scientific and methodological conference dedicated to the 75th anniversary of Professor E.Y. Bidaybekov and the 35th anniversary of school informatics: Mathematical modeling and information technology in education and science. - Abay KazNPU, 2020.
2. Bosova L.L. About new approaches to the study of school informatics in the conditions of digital transformation of society. // Informatics in school. 2022 № 4(177) – p. 3.
3. The Civil Code of the Russian Federation from November 30, 1994 № 51-FZ https://www.consultant.ru/document/cons_doc_LAW_5142/.
4. Doctrine of information security of the Russian Federation". Approved December 5, 2016 № 646. https://www.consultant.ru/document/cons_doc_LAW_208191/
5. Unified Register of Russian Programs for Electronic Computing Machines and Databases. https://www.ispring.ru/software-registry/
6. Kalinin I. A., Samylkina N. N. Informatics. Advanced level. 11th grade. MOSCOW: BINOM. Laboratory of Knowledge, 2013. 216 c.
7. National Program "Digital Economy of the Russian Federation". http://government.ru/info/35568/.
8. Sample working program of the secondary general education subject "Informatics" (basic level). Approved by the decision of the Federal Educational

рального учебно-методического объединения по общему образованию, протокол 7/22 от29.09.2022 г. https://edsoo.ru/Primernaya_rabochaya_programma_srednego_obschego_obrazovaniya_predmeta_Informatika_.htm
9. Примерная рабочая программа среднего общего образования предмета «Информатика» (углубленный уровень). Одобрена решением федерального учебно-методического объединения по общему образованию, протокол 7/22 от29.09.2022 г. https://edsoo.ru/Primernaya_rabochaya_programma_srednego_obschego_obrazovaniya_predmeta_Informatika_uglublennij_uroven.htm
10. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Утверждена Указом Президента России № 203 от 9 мая 2017 г. https://www.consultant.ru/document/cons_doc_LAW_216363/
11. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006г. № 149-ФЗ http://www.consultant.ru/document/cons_doc_LAW_61798/#dst59
12. Федеральный закон «О рекламе» от 13.03.2006 N 38-ФЗ. https://www.consultant.ru/document/cons_doc_LAW_58968/

and Methodological Association for General Education, Minutes 7/22 of 29.09.2022. https://edsoo.ru/Primernaya_rabochaya_programma_srednego_obschego_obrazovaniya_predmeta_Informatika_.htm
9. Sample working program of the secondary general education subject “Informatics” (advanced level). Approved by the decision of the Federal Educational and Methodological Association for General Education, Minutes 7/22 of 29.09.2022 https://edsoo.ru/Primernaya_rabochaya_programma_srednego_obschego_obrazovaniya_predmeta_Informatika_uglublennij_uroven.htm.
10. Strategy for the Development of Information Society in the Russian Federation for 2017-2030. Approved by the Decree of the President of Russia No. 203 of May 9, 2017 https://www.consultant.ru/document/cons_doc_LAW_216363/
11. Federal Law “On Information, Information Technologies and Protection of Information” dated 27.07.2006 No. 149-FZ http://www.consultant.ru/document/cons_doc_LAW_61798/#dst59
12. Federal Law “On Advertising” dated 13.03.2006 N 38-FZ. https://www.consultant.ru/document/cons_doc_LAW_58968/

Программа дополнительного образования детей

В Санкт-Петербурге апробируется и запущен в тестовом режиме проект на получение социальных сертификатов на дополнительное образование для детей и начался прием заявлений. Бесплатный сертификат предполагает посещение ребенком краткосрочного 12-часового курса обучения и не дублирует уже имеющиеся программы.

Предполагается, что в этом году сертификаты получат не менее 171 тысячи ребят - то есть не менее четверти от общего числа петербуржцев в возрасте от 5 до 17 лет. Сертификат выдается на любого ребенка этого возраста, имеющего прописку в Петербурге. Справки о доходах семьи не требуется.

Большинство курсов предлагаются на время осенних каникул, когда у детей много свободного времени. Главная цель нововведения - дать возможность ребенку попробовать свои силы в том или ином направлении, понять, насколько оно интересно и нужно ли им заниматься в дальнейшем. То есть, например, занимается ребенок серьезно музыкой, а по сертификату он может пройти курс, связанный с компьютерной грамотностью, химией, биологией. Есть курсы, предполагающие дополнительные компетенции в рамках уже работающих кружков.

В проекте (по сведениям Комитета по образованию Санкт-Петербурга) задействовано 3700 программ из почти 700 учреждений сферы образования, не только государственных, но и частных. Главное правило - учреждение должно иметь соответствующую лицензию именно на оказание образовательных услуг. Например, конно-спортивный или фитнес-клуб участвовать в проекте не может. То есть если ребенок за деньги родителей занимается конным спортом, то не удастся перевести даже часть занятий на бесплатный сертификат.

Самому учреждению такие программы выгодны материально. Финансирование государственное, а не за счет родителей.

Оформляется сертификат через портал «Госуслуги» (дети с 14 лет могут сделать это самостоятельно). Далее нужно выбрать конкретную программу на навигаторе дополнительного образования Санкт-Петербурга. На следующий год сертификат нужно будет оформлять снова.

(Источник: https://rg.ru/)