Департамент культуры Администрации Владимирской области Департамент

образования Администрации Владимирской области

Государственное бюджетное учреждение культуры Владимирской области
«Владимирская областная библиотека
для детей и молодежи»

Государственное автономное образовательное учреждение
дополнительного профессионального образования Владимирской области
«Владимирский институт развития образования
имени Л.И. Новиковой»

Владимирский государственный университет имени
А.Г. и Н.Г. Столетовых

«ДИАЛОГ-ONLINE»
IX МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Материалы конференции

18 февраля 2021 года

Владимир
2021

УДК 004.056
ББК 78.38
Д 44

Печатается по решению
РИС ВИРО имени Л.И.Новиковой

Ответственный за выпуск:
Т.А. Сдобникова, директор Владимирской областной библиотеки для детей и молодёжи

Редакционная коллегия:
Д.В. Мишин, к.т.н., заведующий кафедрой ЦОИБ ГАОУ ДПО ВО ВИРО (отв. ред.)
А.И. Кондратьева, лаборант кафедры ЦОИБ ГАОУ ДПО ВО ВИРО (техн. ред.)

Диалог-online : материалы IX Межрегиональной научно-практической конференции, 18 февраля 2021 г. / Департамент культуры администрации Владимирской области, Владимирская областная библиотека для детей и молодежи ; Департамент образования администрации Владимирской области, Владимирский институт развития образования имени Л.И. Новиковой ; ответст. за выпуск Т.А. Сдобникова ; редкол.: Д.В. Мишин, А.И. Кондратьева. - Владимир, 2021. - 100 с.

ISBN *-*-******-**-***

Предлагаемый читателю сборник содержит материалы IX Межрегиональной конференции (18 февраля 2021 года, г.Владимир) «ДИАЛОГ-ONLINE». Тематики представленных работ освещают актуальные вопросы безопасности в глобальной информационной среде.

В рамках конференции были рассмотрены следующие вопросы: противоправное использование ресурсов сети Интернет, регулирование информационной сферы, влияние современных инфокоммуникационных технологий на образ жизни, на воспитание и личностное становление подрастающего поколения.

Тексты статей печатаются в авторской редакции.

ISBN *-*-******-**-***

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

Татьяна Алексеевна СДОБНИКОВА,
директор Владимирской областной библиотеки для детей и молодёжи, член Общественной Палаты Владимирской области.

Виктория Александровна ПОЛЯКОВА, к.п.н.,
проректор по информатизации Владимирского института развития образования им. Л.И. Новиковой.

Михаил Юрьевич МОНАХОВ, д.т.н.,
профессор Владимирского государственного университета им. А.Г. и Н.Г. Столетовых, заведующий кафедрой информатики и защиты информации.

Денис Вячеславович МИШИН, к.т.н.,
заведующий кафедрой цифрового образования и информационной безопасности Владимирского института развития образования им. Л.И. Новиковой.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Сборник составлен по итогам VIII Межрегиональной научно-практической конференции «Диалог-online», состоявшейся 27 февраля 2020 года по теме «Актуальные вопросы безопасности в глобальной информационной среде». Конференция была организована Владимирской областной библиотекой для детей и молодежи в рамках государственной программы Владимирской области «Обеспечение информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции во Владимирской области».

Конференцию активно поддержали департамент культуры администрации Владимирской области, департамент образования Владимирской области, Владимирский институт развития образования имени Л.И. Новиковой, Владимирский государственный университет имени А.Г. и Н.Г. Столетовых.

Очевидно, что необходимость популяризировать знания о безопасном поведении в сети «Интернет» с каждым годом становится все более актуальной. Ежегодно в феврале по всей России проходят мероприятия, посвященные безопасному Рунету. Активно включаются в эту работу библиотеки. Их сайты предоставляют пользователям безопасный качественный контент, проводят познавательные мероприятия и кибердиктанты. Библиотеки стремятся научить родителей правильно обеспечивать сетевую безопасность детей, рассказывают им о полезных ресурсах, объясняют, как можно использовать Интернет в обучении, образовании и воспитании.

В конференции приняли участие работники муниципальных библиотек Владимирской области, педагоги, психологи, студенты, ведущие специалисты в сфере IT-технологий, а также представители государственного учреждения культуры "Донецкая республиканская библиотека для молодежи", государственного казённого учреждения культуры «Пензенская областная библиотека для детей и юношества».

Широкий круг участников дал возможность с разных сторон рассмотреть вопросы информационной безопасности, угрозы, с которыми можно столкнуться в Интернете и способы защиты от них.

В ходе работы конференции в пленарном заседании и трех тематических секциях участники выслушали и обсудили свыше двадцати сообщений и докладов по самым актуальным вопросам безопасности в современной глобальной информационной среде.

Конференция послужила усилению координации и межведомственного взаимодействия по созданию безопасной информационной среды, выработке эффективных мер по созданию привлекательного для детей и молодежи положительного онлайн-контента.

СТРАТЕГИИ РОДИТЕЛЬСКОЙ МЕДИАЦИИ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТА ДОШКОЛЬНИКАМИ (5-7 ЛЕТ) И МЛАДШИМИ ШКОЛЬНИКАМИ (8-11 ЛЕТ)

Солдатова Г.У., Теславская О.И.

Повсеместное распространение ИКТ, снижение возраста цифровой инициации, особенности сензитивных периодов дошкольного и младшего школьного возраста, а также высокая значимость родительской позиции в отношении пользования цифровыми устройствами детьми обуславливают необходимость исследования особенностей использования ИКТ в семьях с детьми дошкольного (5-7 лет) и младшего школьного (8-11 лет) возраста. Такое исследование дает не только возможность осознать динамику этого процесса в условиях стремительной цифровизации общества и образования, но и получить важный материал по той группе детей, которые каждый год приходят в начальную школу.

В статье представлена часть результатов, полученных в ходе реализации исследовательского проекта Фонда Развития Интернет при поддержке РФФИ, осуществленного в 2017-2019 гг. В качестве методов использовались полуструктурированное интервью для дошкольников и анкетирование младших школьников и родителей обеих возрастных групп в очной форме на дому у респондентов. Общая выборка - 100 пар «ребенок-родитель» (дети 5-11 лет). Для описания стратегий родительской медиации в работе использована методология проекта EU Kids Online [1].

*Активная медиация (*присутствие и помощь со стороны родителя при использовании ребенком интернета). По совокупности действий по регулированию использования интернета детьми, активная медиация выходит на первый план в семьях с детьми обеих возрастных групп. Родители дошкольников чаще всего контролируют ребенка, присутствуя рядом в то время, пока он пользуется цифровым устройством (70%).Среди родителей младшего школьного возраста это практикуется только в половине семей (52%). Родители младших школьников чаще обсуждают с ребенком его цифровую активность (в 60% семей, в семьях с дошкольниками - 46%) и прибегают к совместным действиям со своим ребенком в онлайн-пространстве (62% в семьях с детьми 8-11 лет, в семьях с дошкольниками - 56%). Целенаправленное обучение использованию интернета также чаще встречается среди семей с детьми младшего школьного возраста (42% у родителей младших школьников и 36% у родителей дошкольников). Родители детей 8-11 лет также гораздо чаще показывают своему ребенку полезные

сайты и рассказывают о пользе интернета в целом - в данной возрастной группе это почти половина родителей (48%), а среди родителей дошкольников - только треть (32%).

*Ограничивающая медиация (*создание родителями правил и ограничений пользования интернетом). Крайне малое количество семей допускает полную вседозволенность в отношении использования детьми интернета (6% в обеих возрастных группах). Однако на вопрос о том, устанавливаются ли конкретные правила относительно использования интернета, утвердительно ответил только каждый пятый (20-22%) родитель детей обеих возрастных групп. На основании таких данных можно предположить, что в большинстве российских семей с детьми дошкольного и младшего школьного возраста медиация использования цифровых устройств носит скорее ситуативный, нежели систематичный характер: родители могут не устанавливать и не обсуждать с ребенком некий свод правил и ограничений относительно использования интернета, а регулировать его непосредственно по мере возникновения необходимости. В ситуации с дошкольником это может случаться, когда родитель занят своим делом, но вдруг вспоминает, что его ребенок уже "слишком долго" играет на планшете. У школьников наиболее частая ситуация - когда ребенок еще не принес родителю на проверку свое домашнее задание, и при этом родитель замечает, что он играет в онлайн-игру.

Характер устанавливаемых правил имеет свою специфику в зависимости от возраста. В семьях с детьми 5-7 лет родители в четверти случаев устанавливают запреты на использование цифрового устройства без участия взрослых (26%), а также прибегают к запретам на определенный вид цифровой активности (4%). Для семей с детьми 8-11 лет эти виды запретов нехарактерны. Родители дошкольников также чаще пользуются запретом на использование цифрового устройства в определенном месте (на кухне, на улице, в транспорте, в общественных местах). Он встречается в каждой четвертой семье с дошкольниками (24%) и менее чем в каждой пятой (18%) - с младшими школьниками. В свою очередь, родители младших школьников гораздо чаще прибегают к временным лимитам на использование детьми цифровых устройств, нежели родители детей 5-7 лет - это делается в двух семьях с детьми 8-11 лет из трех (64%), и примерно в каждой второй семье с детьми младшего возраста (46%). В семьях с детьми младшего школьного возраста существенно чаще можно встретить запрет на использование цифрового устройства до выполнения определенных видов деятельности (чаще всего это выполнение домашнего

задания, помощь родителям по хозяйству, прием пищи и др.) - в половине случае (54%), а в семьях с детьми младшего возраста - только в трети случаев (32%). Кроме того, родители детей 8-11 лет существенно чаще запрещают своим детям пользоваться интернетом - такое предельно жесткое ограничение может устанавливаться в трети опрошенных семей с детьми 8-11 лет (34%) и в одной из пяти семей с детьми 5-7 лет (22%).

*Активная медиация безопасности (*общение родителя с ребенком о безопасном поведении в интернете, включая советы и обучение тому, как правильно себя вести). Помощь ребенку в ситуации столкновения с онлайн-рисками гораздо больше характерна для родителей маленьких детей (5-7 лет). Они чаще обсуждают ситуацию с ребенком и объясняют ему, как поступить в ситуации цифровой угрозы. С другой стороны, для родителей младших школьников существенно более характерно обучение ребенка поведению по отношению к другим людям в интернете (20%), и совершенно несвойственно родителям дошкольников, поскольку их дети не имеют личных аккаунтов в социальных сетях и в виртуальном пространстве общаются только с ближайшими родственниками, как правило, в присутствии и при участии самих родителей. Каждый пятый родитель ребенка 5-7 лет (22%) и 16% родителей детей 7-11 лет устанавливали на компьютер фильтры или программы родительского контроля, а 6% взрослых (независимо от возрастной подгруппы) запрещали пользоваться интернетом после негативной ситуации. Только чуть больше половины родителей детей младшего школьного возраста (54%) и чуть меньше (46%) - родителей дошкольного возраста - считают, что абсолютно все проблемы, возникающие в интернет-пространстве, требуют их вмешательства и контроля.

*Мониторинг (*постоянная проверка родителем сайтов, которые посещает ребенок, его контактов, сообщений, профилей). В применении стратегии мониторинга очевидна возрастная специфика - поскольку именно в младшем школьном возрасте дети начинают активно интересоваться общением в интернете и даже регистрируют свои аккаунты, их родители начинают добавлять ребенка в друзья в социальных сетях (18%), в то время как перед родителями дошкольников этот вопрос пока не стоит. В целом в семьях с детьми обеих возрастных групп примерно в трети случаев (36-40%) родители следят за тем, какие сайты посещает их ребенок. Отметим, что, согласно данным интервью с детьми 5-7 лет, в процессе применения стратегии мониторинга существенная роль отводится отцу, хотя в целом ключевая роль в регулировании

деятельности ребенка онлайн, безусловно, принадлежит матери. Почти в четверти случаев именно отец наблюдает за процессом закачки программ и установки приложений, следит за тем, какие страницы и сайты посещает ребенок.

*Технический контроль (*использование родителем специальных программ, которые позволяют блокировать и фильтровать сайты, отслеживать посещенные сайты или устанавливать ограничения на время пользования). К техническому контролю прибегает почти каждая пятая семья с детьми из обеих возрастных групп (18%). При этом родители дошкольников немного чаще, чем родители младших школьников ставят на компьютер фильтры или программы родительского контроля именно в ситуации столкновения с рисками (22% и 16% соответственно). У большинства родителей средства технической защиты отсутствуют, либо установлены по умолчанию, и взрослые не пользуются ими активно.

В целом родители дошкольников и младших школьников не различаются по субъективной уверенности в том, насколько могут помочь ребенку в освоении интернета, а также по большинству стратегий родительской медиации. Родители чаще говорят с младшими школьниками о том, как вести себя по отношению к другим людям онлайн: в нашей выборки об этом говорит каждый пятый родитель младших школьников и ни одного родителя дошкольников (χ^2=11,11, p<0,01, Cramer'sV=0,33). Каждый шестой родитель младших школьников добавляет их в друзья в социальной сети, тогда как в дошкольном возрасте таких ответов не было (χ^2=9,89, p<0,01, Cramer'sV=0,31).

Одинаково часто родители используют большинство ограничений. Основное исключение касается запрета использовать цифровое устройство без родителей: его не отметил ни один родитель младших школьников и каждый четвертый родитель дошкольников (χ^2=14,94, p<0,01, Cramer'sV=0,39). Наоборот, младшим школьникам чаще, чем дошкольникам нельзя использовать устройство до выполнения каких-либо обязанностей, прогулки и пр. (χ^2=4,94, p<0,05, Cramer'sV=0,22).

Говоря о стратегиях родительской медиации, нельзя не упомянуть о том, что, вопреки распространенным жалобам родителей и воспитателей, дети хотят проводить время со взрослыми офлайн. Когда мы попросили детей назвать свое любимое офлайн-занятие и предложили выбор между ним и игрой на цифровом устройстве (Вопрос: «Если бы тебе предложили на выбор поиграть в [название любимого устройства] или в [название

обычной любимой игры], что бы ты предпочел(ла)?»), большинство (59%) дошкольников выбрало обычную игру. Дети хотели бы сыграть в прятки, догонялки, крестики-нолики, шахматы. Они были бы рады научиться готовить или почитать, отправиться на прогулку, в зоопарк или кататься на лошадях, устроить дискотеку, провести опыты по химии или заняться выжиганием по дереву. Наконец, дети с нетерпением ждут родительских отпусков (Детские цитаты: «Папа показывал в Таиланде карты, и мы смотрели там много картинок», «Хотел бы остаться с родителями на ночь в лесу», «Мечтаю полететь на море»). Более того, даже среди тех детей, которые больше интересуются электронными видами активностей, многие на самом деле связаны с реальной жизнью. Дети упомянули о том, что с удовольствием сходили бы с семьей в кино, посмотрели вместе мультфильмы или телевизор, сфотографировались с родителями. Такие ответы детей, очевидно, свидетельствуют о том, что для эффективной медиации поведения ребенка в интернете недостаточно только лишь требования от ребенка выполнять установленные родителями правило, необходимо предлагать детям интересные альтернативные способы времяпрепровождения, в которые будут активно вовлекаться и сами родители.

Исследование выполнено при финансовой поддержке РФФИ в рамках проекта № 20-013-00857 А.

Список источников:

1. Livingstone S., Haddon L., Gorzig A., Olafsson K. Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9—16 year olds and their parents in 25 countries. L.: EU Kids Online Network, 2011.

СЕМЕЙНАЯ ЛЕТОПИСЬ: ЭЛЕКТРОННЫЕ РЕСУРСЫ ПО ПОИСКУ РОДСТВЕННИКОВ-УЧАСТНИКОВ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ

Андреева Т.Г.

С каждым годом ветеранов Великой Отечественной войны становится все меньше, и скоро наши дети смогут узнать о подвиге поколения наших дедушек и бабушек только из уроков истории. В то же время, с развитием интернета появилось больше возможностей воссоздать и сохранить историю этого всенародного подвига.

На сегодняшний день в Рунете существует множество ресурсов о Великой Отечественной войне: от уникальных архивов до мультимедийных карт военных действий, от сборников видеоинтервью ветеранов до семейных фотоальбомов.

Если вы интересуетесь историей своей семьи – сайты по поиску родственников-участников Великой Отечественной войны должны вам помочь. В сети Интернет существует множество баз данных, куда ежегодно выкладываются миллионы копий военных документов, свидетельств, карт и новых данных о местах захоронений жертв Великой Отечественной войны.

Поиск такой информации – большая и кропотливая работа. Нужно учитывать, что запрашивать официально информацию о человеке в Архивах и учреждениях Министерства обороны могут только родственники или государственные учреждения (военкоматы, администрации, органы полиции и ФСБ, Госархивы) и, в некоторых случаях – общественные организации социальной направленности.

Победа в Великой Отечественной войне досталась стране очень дорогой ценой. Судьбы тысяч людей так и остались невыясненными. До сих пор продолжаются поиски мест захоронений погибших воинов. С целью организации работы по увековечению памяти павших защитников Отечества и реализации на практике лозунга «Никто не забыт, ничто не забыто» Президент Российской Федерации издал ряд поручений и Указов.

В соответствии с Перечнем поручений Президента Российской Федерации от 23 апреля 2003 г. № пр-698 по вопросам организации военно-мемориальной работы в Российской Федерации и Указом от 22 января 2006 года № 37 «Вопросы увековечения памяти погибших при защите Отечества», Министерством обороны Российской Федерации был создан **Обобщенный компьютерный банк**

данных, содержащий информацию о защитниках Отечества, погибших и пропавших без вести в годы Великой Отечественной войны, а также в послевоенный период (**ОБД Мемориал**).

Главная цель проекта – дать возможность миллионам граждан установить судьбу или найти информацию о своих погибших или пропавших без вести родных и близких, определить место их захоронения.

На сайте можно найти информацию о звании погибшего, части, в которой он служил, дате и причине смерти (убит, умер от ран, пропал без вести) и месте захоронения. Более того, на сайте выложены отсканированные копии всех обработанных документов-первоисточников, содержащих информацию о персоналиях. Эти документы позволяют с большой точностью идентифицировать павших, поскольку в них часто содержится дополнительная информация, в частности имена и адреса родственников, которым отсылались похоронки.

В рамках проекта отсканировано и предоставлено в Интернет-доступ более 13 миллионов листов архивных документов и свыше 30 тыс. паспортов воинских захоронений. Впервые можно ознакомиться с реальными документами, самостоятельно провести поиск и исследование.

На сегодняшний день ни в одной стране мира нет подобного банка данных.

Сайт «Подвиг народа» - уникальный информационный ресурс открытого доступа Министерство обороны Российской Федерации, наполняемый всеми имеющимися в военных архивах документами о ходе и итогах основных боевых операций, подвигах и наградах всех воинов Великой Отечественной.

Основными целями проекта являются увековечение памяти всех героев Победы, военно-патриотическое воспитание молодежи на примере военных подвигов отцов, а также создание фактографической основы для противодействия попыткам фальсификации истории Войны.

Портал «Память народа», создан Министерством обороны по решению Российского оргкомитета «Победа» и поддержан поручением Президента Российской Федерации и Постановлением Правительства РФ. Главная цель проекта – предоставить возможность пользователям получить наиболее полную информацию об участниках Великой Отечественной войны за счет

новых интерактивных инструментов и развития обобщенных банков данных «Мемориал» и «Подвиг народа в Великой Отечественной войне 1941-1945 гг.».

В рамках проекта «Память народа» впервые оцифровано и выложено в Интернет 425 тысяч архивных документов фронтов, армий и других соединений Красной Армии. Это документы о ходе боевых действий, приказы, доклады командующих, оперативные описания боевой обстановки. Кроме того, отсканированы и систематизированы более 100 тысяч военных карт. Изучение этих документов позволяет восстановить героический путь каждого из участников Войны – от призыва до возвращения домой.

Строчки из наградных листов с описаниями подвигов, представлений к наградам – это самые красноречивые свидетельства судеб солдат и офицеров. Таких записей на портале «Память народа» – более 18 миллионов. Описания подвигов, обстоятельства их совершения – очень ценная информация для потомков Героя.

На **сайте «Бессмертный полк»** хранятся данные об участниках боевых действий и тружеников тыла – живых, умерших, пропавших без вести. Их собирают и пополняют участники ежегодной акции «Бессмертный полк»: в каждом городе колонны из сотен и тысяч родственников собираются, держа в руках транспаранты с фотографиями и именами родственников, заставших войну, и проходят бессмертным полком по главным улицам своих городов. На странице Владимирской области, города Владимир собрано 1600 историй наших земляков. Если совсем не знаете с чего начать, именно этот сайт расскажет и покажет, как работать с поисковым аппаратом. И у каждого есть возможность добавить историю своего деда, прадеда к этому архиву.

Добровольческий проект «Архивный батальон» по восстановлению сведений об участниках войн XX века направлен на увековечивание памяти погибших при защите Отечества и сохранение в семьях памяти об участниках Великой Отечественной войны, в том числе пропавших без вести. Проект стартовал в сентябре 2015 года и очень быстро набрал популярность, ежегодно поступают тысячи заявок на исследование боевого пути. Подача заявки происходит по принципу «одного окна» (родственники подают заявку на исследование боевого пути в «Архивный батальон» по горячей линии или лично), а всю исследовательскую работу проводят специалисты и добровольцы, осуществляющие

поиск на десятках интернет-ресурсов и путём запросов информации в российских и зарубежных архивах.

Сайт «Солдат» – электронная библиотека книг памяти (по отдельным регионам и родам войск, воинским частям и соединениям). Найти здесь можно сведения не только о родственниках – участниках Великой Отечественной войны, но и о воевавших и погибших в Афганистане и Чечне.

Пользоваться сайтом довольно легко: выбираете книгу памяти по интересующему региону, в отдельно открытой строке вводите ФИО родственника, год рождения и место призыва (если оно вам известно).

База данных центра документации при Объединении **«Саксонские мемориалы»** (Дрезден) доступна онлайн на немецком и русском языке. В ней собрана информация о советских военнопленных, находившихся в лагерях или в рабочих батальонах на территории рейха. Интернет-архив содержит данные о примерно 700 тысячах военнопленных Второй мировой войны, большая часть которых погибла в немецком плену. Обнародованная база данных включает в себя базовую информацию: имена и фамилии военнопленных, дату рождения и дату смерти. Однако пользователи, которые найдут в списке имена своих близких, могут обратиться к исследователям с запросом для получения более детальной информации. Эти архивы помогут миллионам людей узнать судьбу своих погибших или пропавших без вести родственников.

Всенародный исторический депозитарий «Лица Победы» создан на базе московского Музея Победы. Всенародный исторический депозитарий – это более 150 миллионов фото и текстовых документов, более 150 миллионов судеб. В Музее Победы создана «народная экспозиция», в которой участники проекта «Лица Победы» могут найти портрет своего предка и показать его своим детям и внукам. Проект имеет международный статус, граждане любой страны могут внести сведения о своих близких в исторический депозитарий в Музее Победы и увековечить подвиг поколения, победившего нацизм. Любой желающий может передать материалы из своего семейного архива в исторический депозитарий в Музее Победы. Это можно сделать через сайт, мобильное приложение, отправить по почте или лично принести в музей на площади Победы в Москве.

Проект «Победители» разработан творческой рабочей группой, собранной Яном Черняком вокруг студии «Web-Мастерская». Цель проекта: «Нашим проектом мы хотим поименно поблагодарить живущих рядом с нами солдат Великой Отечественной войны и рассказать об их подвиге». Проект был сделан весной 2005 года – к 60-летию Великой Победы.

В «Победителях» две главные части. Более наглядная – это интерактивная мультимедийная карта боевых действий Великой Отечественной войны. Все основные события с 22 июня 1941 до 9 мая 1945 показаны на карте, снабжены фото- и кинохроникой, воспоминаниями в аудиоформате, архивными документами – непрерывная презентация длится почти пять часов. Кроме того, на сайте есть база данных с именами живущих в России ветеранов – их более миллиона. Хроника войны пополнялась уже после открытия проекта, работа была завершена к юбилею Победы. Пофамильный список ветеранов Владимирской области составляет 11587 имен.

Владимирская областная библиотека для детей и молодёжи предлагает помощь в использовании электронных ресурсов при поиске информации о родственниках-участниках Великой Отечественной войны, в выявлении и установлении фронтовой судьбы родных и близких, погибших и пропавших без вести в годы Великой Отечественной войны 1941–1945 годов.

Определите всю информацию, которую вы знаете о разыскиваемом человеке: фамилию, имя, отчество, дату и место рождения, место проживания до войны, место и дату призыва в ряды РККА, фамилии, имена и место проживания близких родственников (отец/мать, брат/сестра, муж/жена, т.е., кого мог указать в качестве близкого родственника для извещений). Расспросите родных, близких, знакомых – соберите как можно больше информации. Посмотрите в домашних архивах документы – письма, извещения, справки, фотографии (особенно надписанные), военный билет, партбилет и т.д.

Объединение всех данных электронных ресурсов даст возможность людям самим искать документы, создавать личные архивы, изучать обстоятельства и трагические моменты боевых действий.

Список источников:

1. Мемориал : обобщенный банк данных / Министерство обороны Российской Федерации. - URL: https://obd-memorial.ru/html/ (26.03.2020).

2. Подвиг народа в Великой Отечественной войне 1941-1945 гг. : электронный банк документов / Министерство обороны Российской Федерации. - URL: http://podvignaroda.ru/?#tab=navHome (26.03.2020).

3. Память народа : портал / Министерство обороны Российской Федерации. - URL: https://pamyat-naroda.ru/ (26.03.2020).

4. Бессмертный полк : [официальный сайт ; дислокация полка: Владимирская область, Владимир]. - URL: https://www.moypolk.ru/ (26.03.2020).

5. Архивный батальон : добровольческий проект по исследованию боевого пути участников Великой Отечественной войны. - URL: https://myveteran.ru/ (26.03.2020).

6. Солдат.ru : электронная библиотека Книг памяти. - URL: http://www.soldat.ru/links/?group=3 (26.03.2020).

7. Саксонские мемориалы : база данных центра документации при Объединении «Саксонские мемориалы», Дрезден. - URL: www.dokst.ru (26.03.2020).

8. Лица Победы : всенародный исторический депозитарий / Музей Победы. - URL: https://historydepositarium.ru/ (26.03.2020).

9. Победители : проект / Студия веб-дизайна «Web-Мастерская» ; Ян Черняк. - URL: https://www.pobediteli.ru/ (26.03.2020).

ПОЗНАВАТЕЛЬНАЯ ИГРА «Я НИКОГДА НЕ…»

Некрасова С.В.

Цель игры: сформировать у подростков знания по безопасному использованию интернета, популяризировать их в сети интернет, поднять престиж библиотечных услуг, развить личностные качества учащихся: чувство ответственности за свои действия.

Оборудование: штрафные фишки, коробка для листков с утверждениями, компьютер или мобильные телефоны с доступом в Интернет.

Участники: учащиеся средних и старших классов.

Время проведения игры: 30 мин.

Место проведения: учебная аудитория или библиотека.

Условия игры.

Участникам предлагается случайным образом выбрать одно утверждение из перечня, вытащив его из коробки. Все эти утверждения являются правилами безопасного использования Интернета. Участник произносит фразу «Я никогда не…» и зачитывает вслух утверждение. Если он делал то, что прочитал когда-либо, ему присуждается штрафное очко. В процессе игры, ведущий может комментировать правила и разъяснять их.

По результатам игры, участники, которые набрали штрафные баллы, должны выполнить задания (или одно из них):

1. Подписаться на группу/страницу библиотеки.
2. Сделать запись на своей странице в социальной сети со списком правил безопасности в Интернете.
3. Написать на своей странице в социальной сети о том, какие правила безопасности в интернете он нарушает и почему этого нельзя делать.
4. Снять 30-секундное видеообращение к сверстникам о том, почему нужно быть внимательным и осторожным в Интернете.

Перечень утверждений

1) …пересылал конфиденциальную информацию (номер банковской карты, ПИН-код, паспортные данные) через мессенджеры социальных сетей.

Разъяснение. Письма со сканами документов лучше удалять сразу после отправки или получения, не надо хранить их в почте.

2) … оставался на своей странице в социальных сетях или на почте (разлогинивался), когда пользовался чужим компьютером.

3) … оставлял включенным Wi-Fi, когда им не пользовался.

4) … подключался к беспарольным Wi-Fi – соединениям.

Разъяснение. Чаще всего именно такие сети злоумышленники используют для воровства личных данных пользователей.

5) … заходил в онлайн-банки и другие важные сервисы через открытые Wi-Fi-сети в кафе или на улице.

Разъяснение. В таком случае, воспользуйтесь мобильным интернетом.

6) … переходил по ссылке из письма от банков, сервисов и магазинов с просьбой изменить свой пароль, ввести номер банковской карты и секретный код подтверждения или сообщить другие личные данные.

7) … пользовался одним и тем же электронным адресом для личных целей, работы и сервисов.

8) … использовал простой пароль или использовал один пароль для всех социальных сетей и электронной почты.

9) … отказывался от обновления антивирусной программы.

Разъяснение. Устаревшие версии не могут гарантировать защиту от вредоносного ПО. Ежедневно в мире появляется несколько новых вирусов, поэтому антивирусу нужно как можно чаще получать информацию о методах борьбы с ними.

10) … кликал по ссылкам, пришедшим в сообщениях от незнакомых людей.

Разъяснение. Это верный способ попасться на удочку кибермошенников и заразить свое устройство вирусами. Опасная ссылка может прийти и от взломанного знакомого, поэтому лучше уточните, что такое он вам прислал и нужно ли это открывать.

11) … запускал неизвестные файлы, особенно с расширением .exe

12) … отвечал на спам.

13) … отправлял деньги, если получал на мессенджер просьбу от знакомого о помощи.

Разъяснение. Сначала перезвоните ему и удостоверьтесь, что аккаунт не был взломан злоумышленниками.

14) … публиковал в сети домашний адрес, писал, в какое время вас не бывает дома, описывал свой постоянный маршрут, хвалился крупными покупками и афишировал уровень достатка.

15) … пользовался одним и тем же паролем несколько лет.

16) … сохранял важный документ в одном экземпляре.

Разъяснение. Регулярно выполняйте резервное копирование данных. Следуйте правилу «3-2-1»: создайте одну основную копию и две резервные. Сохраните две копии на разных физических носителях, а одну — в облачном хранилище (Google Диск, Яндекс.Диск, специальные решения от Акронис).

17) … указывал девичью фамилию матери, которая сейчас есть в открытом доступе на ее страницах в соцсетях в секретном вопросе.

18) … замалчивал родителям о непонятной информации, которую нашел в интернете.

19) … скачивал сомнительные приложения и пытался это делать по неизвестным ссылкам.

20) … делал покупки с предоплатой через социальные сети.

Разъяснение. Постарайтесь ничего не покупать в социальных сетях, особенно с предоплатой. Мы вообще не рекомендуем переводить деньги на карту физических лиц (то есть, когда кто-то просто дает вам номер или реквизиты своей карты).

21) … покупал в интернет-магазинах товары по сильно заниженной цене.

22) … доверял отзывам по шаблону в интернет-магазине.

23) … использовал одну карту для платежей в интернете и других трат.

24) … отключал смс-информирование от банка об операциях.

Разъяснение. При смс-информировании вы сможете быстро заметить, если ваша карта будет скомпрометирована, и заблокировать ее.

25) … общался на личные темы с незнакомцами, делился с ними секретами и переживаниями.

Разъяснение. Будьте осторожны при общении в сети с незнакомыми, они могут оказаться не теми, за кого себя выдают.

26) … доверял сообщениям о многомиллионном выигрыше или получении наследства от неизвестных богатых родственников.

27) … делал репосты «жалостливых» объявлений про милого котика, который срочно ищет дом, если в посте был телефон владельца или номер карты, куда можно перечислить деньги на содержание животного.

Разъяснение. Велика вероятность, что это мошенники, решившие заработать на сердобольных и доверчивых гражданах.

28) … доверял логотипам известного благотворительного фонда в объявлении, не проверяя информацию.

Разъяснение. Реквизиты счета могут быть подделаны. Если хотите помогать людям, делайте это только для лично знакомых.

29) … заходил на сайты, не смотря на отличие в адресе страницы от требуемого.

Разъяснение. Обращайте внимание на адрес страницы, где вы оказались: если он отличается хотя бы на один символ (например, paypa1.com вместо paypal.com), введите его вручную самостоятельно.

30) … пользовался торрентами.

Разъяснение. Если вы скачиваете нелегальный контент, вы не только обкрадываете любимого автора, но и можете загрузить зараженный вирусом файл.

31) … отправлял номер телефона или отправлял сообщение на короткий номер для того, чтобы бесплатно посмотреть или скачать приглянувшийся фильм

Разъяснение. Так с вашего счета могут списать внушительную сумму за СМС, а сам телефон попадет в базу спамеров.

32) … участвовал в акциях с призами, где надо что-то оплатить, а потом попросить сделать то же самое еще нескольких людей.

33) … оставлял компьютер без блокировки, если отходил от него в общественном месте.

34) … ставил метку о своем местоположении в социальных сетях.

35) … отправлял незнакомым людям свои фотографии по их просьбе.

ВЕБКВЕСТ КАК ФОРМА БЕЗОПАСНОГО ИНТЕРНЕТА В УСЛОВИЯХ ГЛОБАЛЬНОЙ ИНФОРМАЦИОННОЙ СРЕДЫ

Почаева Н.Д.

Как обеспечить безопасность в интернете...

Интернет уже давно стал незаменимым помощником современного человека. Всемирная сеть является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Именно поэтому дети активно пользуются интернетом, а зачастую проводят в Сети даже больше времени, чем взрослые. Юные пользователи осваивают сервисы мгновенных сообщений и интернет-телефонию, общаются на форумах и в чатах, каждый день узнают много увлекательной образовательной информации. Однако не стоит забывать, что интернет может быть не только средством для обучения, отдыха или общения с друзьями, но – как и реальный мир – Сеть тоже может быть опасна. Чтобы быть подготовленным к опасностям, нужно знать о них.

Перед педагогами стоит задача, как сделать процесс изучения нового увлекательным и полезным.

Согласно исследованиями психологов, мы запоминаем 10% того, что мы читаем, 20% того, что слышим, 30 % того, что мы видим и слышим, 70% того, что мы говорим, 90% того, что мы говорим и делаем. По словам великого древнего китайского философа:
«Скажи мне – и я забуду; Покажи мне - может быть, я запомню; Вовлеки меня – и я пойму»

Реализовать вышеуказанные принципы позволяет технология веб-квестов. Веб-квест – это отличный вариант организации занятия с использованием компьютерных технологий, который позволяет ученикам или студентам работать в группах или самостоятельно. Учащиеся используют интернет для поиска информации на определенную тему, заданную веб-квестом.

Был создан веб-квест для школьников по информационной безопасности «Опасности net». Подробное описание квеста, можно найти по адресу: https://clck.ru/HeQa3 .

Цель квеста: Знакомство с опасностями в интернете, составление правил безопасного поведения в Сети.

Задачи:

Сформировать знания и умения:

- безопасного использования интернет-пространством;

- работы с веб-сервисами, поисковыми системами;
- анализировать информацию;
- выражать своё мнение;
- творчески создавать продукт;
- работать в команде.

Необходимое ПО и оборудование:

- ноутбук или мобильное устройство с выходом в интернет;
- ручки, бумага.

Продукт деятельности участников.

Презентация с правилами безопасного интернета. Стенгазета. Выступление перед младшими школьниками

Сетевое пространство квеста

- Информационное место, сайт: Вики Владимир http://www.wiki.vladimir.i-edu.ru . образовательный портал, защищенный от ненужного контента;
- Сайт интерактивных обучающих приложений https://learningapps.org ;
- Поисковая система Яндекс https://yandex.ru/ ;
- Место сбора итоговых презентаций на стена совестного редактирования https://padlet.com .

Правила квеста:

- Продолжительность квеста – произвольная (от 1 часа до 1 месяца). За это время нужно выполнить как можно больше заданий и создать презентацию с правилами безопасного поведения в сети интернет;
- Ответы на задания фиксируются в "Блокноте участника квеста";
- Можно пользоваться всеми мобильными устройствами, всеми поисковыми системами;
- Можно выполнять одновременно несколько заданий;
- В команде нужно распределить роли: капитан, копирайтеры, искатели, другие роли вы можете придумать сами, главное, чтобы это шло на пользу команде, фотограф (если хотите оставить на память фото);
- По итогам квеста, участники создают стенгазету по правилам «Безопасного интернета»;

- Участники квеста с презентацией и стенгазетой проводят классный час в младших классах. Стенгазету оставляют в дар школе;
- По итогам проводиться рефлексия.

Задания.

Все задания имеют два уровня. Первый уровень тренировочный, задания к нему размещены на сайте интерактивных обучающих приложений https://learningapps.org . В случае правильного решения тренировочного задания, участникам автоматически предоставляется ссылка на основное задание, ответ на него они размещают в презентации.

Источники информации по безопасному поведению в сети являются видеоуроки:

- Видеоурок для Единого урока по безопасности в сети интернет 2016 https://youtu.be/K1XzMIb-bdE ;
- Видеоурок для Единого урока по безопасности в сети интернет 2017 https://youtu.be/yTCcfc3i5NQ ;
- Безопасность школьников в сети Интернет https://youtu.be/9OVdJydDMbg .

Подробное описание квеста, можно найти по адресу: https://clck.ru/HeQa3 .

Предложенный квест готов к использованию.

Список источников:

1. Понятие «Веб-квест» [Электронный ресурс] // WikiHow : вики-проект. - URL: https://ru.wikihow.com/Заглавная-страница

2. Я НЕУЧ! [Электронный ресурс] : сайт. - URL: http://yaneuch.ru/cat_22/zashhita-personalnogo-kompjutera-rabota-antivirusnyh/379903.2633364.page2.html

ПРОЕКТЫ КООРДИНАЦИОННОГО ЦЕНТРА ДОМЕНОВ .RU/.РФ ПО ПОВЫШЕНИЮ МЕДИАГРАМОТНОСТИ СОВРЕМЕННЫХ ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЕЙ

Новикова Т.И.

Координационный центр национального домена сети интернет – администратор национальных доменов .RU и .РФ, основной миссией которого является развитие национального сегмента сети Интернет, обеспечение целостности, непрерывности, стабильности, устойчивости и защищенности функционирования Рунета.

Кроме этого, Координационный центр содействует повышению безопасности использования интернета, реализуя ряд проектов, направленных на противодействие использованию национальных доменов страны в противоправной деятельности («Нетоскоп», институт Компетентных организаций). Другая значимая составляющая – собственные активности и поддержка партнерских проектов, адресованных начинающим пользователям, способствующих повышению их цифровой грамотности и кибергигиены, что также содействует популяризации российских интернет-сервисов и закреплению навыков безопасного использования сети в целом.

Именно для просвещения начинающих пользователей и повышения их информационной грамотности Координационный центр разрабатывает свои социальные и просветительские проекты, которые позволяют напрямую общаться с учащимися и учителями, прививать им навыки безопасного использования дистанционных сервисов, повышать осведомленность о принципах функционирования интернета и доверие к глобальному информационному пространству.

В 2019 году национальный домен .RU отметил 25-летие. Это событие было поддержано как качественным развитием действующих проектов, так и появлением новых форм взаимодействия с детско-юношеской аудиторией.

Так, среди новых – проект **«Путешествие по RUнету» (https://www.karusel-tv.ru/contest/25RU)**, реализованный совместно с телеканалом «Карусель». Это конкурс рисунков, а также серия видеороликов, рассказывающая детям об устройстве и функционировании сети доступными словами (материалы доступны на сайте телеканала бессрочно).

Также значимым событием 2019 года стали съемки **документального фильма «Интернет для всех» (https://film25.cctld.ru/).** Это альманах из 11 историй людей, жизнь которых качественно изменилась, благодаря цифровым

технологиям. Для одних героев фильма интернет стал социальным лифтом – помог приобрести новые знания и дело своей жизни, другим помог найти семью, расширить круг общения, реализовать экологические проекты и даже прославиться. Премьера фильма состоялась в сентябре 2019 года в московском Доме кино; в ноябре «Интернет для всех» стал фильмом открытия Фестиваля образовательного кино «Взрослеем вместе», который прошел в Челябинске.

Среди долгосрочных проектов, который реализует Координационный центр при поддержке ПАО «Ростелеком», – **«Изучи интернет – управляй им!» (http://игра-интернет.рф/**). Цель проекта - повысить цифровую грамотность пользователей, сократить цифровой разрыв между поколениями, а также развить навыки эффективного использования интернет-технологий. Проект работает с 2012 года. Кроме *интернет-портала с блоком «Знания»,* где в игровой форме (викторины, пазлы, квесты, головоломки) пользователи приобретают базовые знания об устройстве Всемирной паутины, игроки могут скачать *мобильное приложение на смартфон* и продолжить играть в удобное время буквально на бегу. *Лайт-вариантом блока «Знания» можно назвать Викторину*, реализованную в формате популярного телепроекта «Своя игра». Соревновательная составляющая особенно увлекает учеников средней школы. Важная особенность Викторины в том, что она работает даже при неустойчивом интернет-соединении: единожды открыв этот раздел в браузере, можно полноценно работать с ним до тех пор, пока вы не нажмете кнопку выхода.

В рамках проекта «Изучи интернет – управляй им!» также проходит **серия локальных турниров по киберграмотности, ежегодный Семейный IT-марафон и Всероссийский онлайн-чемпионат для школьников**. Последний в 2019 году собрал 17,5 тысяч участников. Каждый участник выполнил 24 интерактивных задания, которые были посвящены доменам, управлению и инфраструктуре доменной индустрии, 25-летию домена .RU.

Среди проектов Координационного центра есть и два нишевых конкурса. Например, **«DOT-журналистика» (http://дот-журналистика.рф/)** - конкурс для профессиональных и начинающих журналистов, которые освещают в своих статьях, аналитических материалах, репортажах тенденции и явления доменной индустрии, ключевые события, связанные с использованием DNS и других систем адресации интернета. Конкурс также ставит перед собой важную задачу популяризировать доменную тематику в среде интернет-пользователей, разъяснить преимущества владения

доменным именем, повысить профессиональный и качественный уровень материалов о системах интернет-адресации и новых технологиях в целом.

Для будущих юристов (старшеклассников и студентов), которые планируют связать свою профессиональную деятельность с интернет-правом, при поддержке Координационного центра проводится **Всероссийский молодежный конкурс работ по праву информационных технологий и интеллектуальной собственности «IP&IT LAW»**. На Конкурс необходимо представить индивидуальное, актуальное и ранее не публиковавшееся исследование, в котором с опорой на законодательство, доктрину, отечественную и зарубежную судебную практику рассматриваются проблемные правовые вопросы, а также даются новые варианты их решения. Среди призов – диплом Всемирной организации интеллектуальной собственности, что является символом признания успехов в области инновационной и творческой деятельности.

Также среди социальных проектов Координационного центра – **кириллический домен .ДЕТИ**, предназначенный для адресации ресурсов детской и подростковой тематики. Все сайты в этой доменной зоне подвергаются круглосуточному мониторингу: любая вредоносная активность и нежелательный для этой чувствительной аудитории контент немедленно блокируются. Лучшие сайты *в .ДЕТИ собраны в тематический каталог (http://интернет.дети/catalog/)* - образовательные и развлекательные, творческие и спортивные, ресурсы о безопасности, детском здоровье и досуге. Среди них: сайт Российской государственной детской библиотеки библиотека.дети, каталог лучших сайтов для детей веб-ландия.дети, просветительский сайт о кибербезопасности касперский.дети, персональныеданные.дети – проект Роскомнадзора о том, как защищать свои персональные данные в интернете и другие.

ПОСЛЕДСТВИЯ ВНЕДРЕНИЯ СРЕДСТВ ЦИФРОВИЗАЦИИ В СРЕДНЕЙ ОБРАЗОВАТЕЛЬНОЙ ШКОЛЕ: ВЗГЛЯД ПЕДАГОГА

Зубанова Е.А., Монахов Ю.М.

Внедрение средств цифровизации в учебных организациях помогает интегрировать в практику урочной деятельности технологию электронного обучения. Это позволяет школьникам создавать проекты, учителям пользоваться интернет-ресурсами и применять наглядные материалы в урочной деятельности. Однако, после внедрения таких средств современные школы сталкиваются со множеством проблем – например, связанных с электронными дневниками, контент-фильтрацией и недостаточной адаптированностью учителей, контингента обучающихся и их родителей к этим нововведениям. С одной стороны, механизмы информационной безопасности позволяют огородить школьников от просмотров нежелательных сайтов, а с другой -- ограничивает возможность применять на уроках видеоматериалы из интернета для наиболее продуктивного обучения, ведь школьникам необходимо не только чтение и слушание учителя, но и визуализация.

Проблемы, связанные с контент-фильтрацией актуальны как для педагогов, так и для учащихся.

Для педагогов актуально в первую очередь то обстоятельство, что зачастую системы контент-фильтрации не обладают достаточной гибкостью при внесении интернет-ресурсов в «черный список» — вместо того, чтобы блокировать конкретные страницы в социальных сетях и определенные видео на хостинге, они блокируют всю социальную сеть или хостинг. В результате теряется возможность использовать общедоступные видео с платформ типа *YouTube*, *Rutube*, «Вконтакте» в качестве учебных и методических пособий, наглядных примеров в урочной и внеурочной деятельности;

Многие преподаватели применяют на уроках не только работу с учебниками и тетрадями, но и пользуются наглядными примерами: презентациями или научными фильмами – к примеру, на уроках музыки для качественного закрепления материала требуется

посмотреть концерт или фрагменты из спектаклей в зависимости от учебного плана. Классным руководителям же работа с цифровым образовательным пространством оказывает значительную помощь при подготовке классных часов.

Авторы замечают, что иногда системные администраторы, опасаясь проверок со стороны регуляторов и надзорных органов, «перестраховываются» и создают вместо «черных» списков фильтрации «белые», куда вносят только минимально необходимый для функционирования информационных систем школы список ресурсов. Эти списки администраторы формируют по своему усмотрению, из соображений, не относящихся ни к учебному процессу, ни к методической работе. В результате эффективность педагогов при подготовке к занятиям радикально снижается, т.к. они не могут пользоваться необходимыми им интернет-источниками.

В отношении учеников же актуален тот момент, что они приходят в школу со своими устройствами, имеющими отдельный канал связи с глобальной сетью. Школа не может контролировать то, к каким ресурсам ученик получает доступ, а ведь нередко учащиеся используют свои мобильные устройства непосредственно на уроках. Школа также не вправе устанавливать «глушилки», препятствующие установлению мобильной связи, а также ПО контент-фильтрации на устройствах учащихся -- это хоть и не относится к техническим проблемам, но сильно влияет на «цифровой климат» в образовательном учреждении. Если мы отключаем интернет или отбираем телефон у ученика, то мы определенным образом нарушаем его права, и как совместить соблюдение прав и безопасность детей в школе, пока неизвестно: этот вопрос остается открытым.

Внедрение электронных дневников и электронных журналов в образовательный процесс также оказалось сопряжено с массой трудностей. Например, со стороны педагогов оно привело к тому, что появилась необходимость заполнять два комплекта документов вместо одного. Более того, неясен статус де-факто этих документов: подчас электронные журналы и дневники получают необоснованный «приоритет» в глазах учащихся и родителей, хотя они скорее всего содержат неактуальную и недостоверную информацию.

Несмотря на то, что все классы оборудованы техникой для доступа в Интернет, из-за плохо функционирующей информационной инфраструктуры в школе (нет доступа к серверам БАРС, неизвестно время восстановления доступа к сети) приходится заполнять журналы в нерабочее время и вне учебного заведения; или же, исходя из практики, есть вариант выставить оценки там, где доступ в интернет качественнее - в кабинете администрации или секретаря, что влечет за собой опоздание на следующий урок, а выставлять оценки учащимся требуется каждый день как в бумажный, так и в электронный журнал.

На текущем уровне развития АИС «Образование» в части электронных дневников не обладает достаточной гибкостью, чтобы в полной мере организовать коммуникацию между педагогом и родителем. Например, функционал электронных дневников не позволяет оставлять заметки о поведении и прилежании ученика, как это часто делается в бумажных дневниках. Психологический эффект от электронных заметок также снижен: сравните, например, «кол» в дневнике красной ручкой и простой набор пикселей на экране смартфона. Также в АИС отсутствует крайне необходимый функционал по оповещению родителей и организации с ними конференцсвязи: в настоящее время классному руководителю приходится для этого использовать сторонние мессенджеры, а неизвестно, насколько они защищены. С появлением интернета в школе, с точки зрения авторов, учителям необязательно собираться на совещания в определенное время -- проводить педсовет можно и дистанционно, ведь есть учителя, которые не могут посещать педсоветы из-за уроков во второй смене.

При проведении открытых уроков в масштабе города не все учителя могут приехать в назначенное время. В таком случае с помощью качественного интернета можно устроить онлайн-трансляцию, но из-за отсутствия качественного интернета в школе это осуществить невозможно.

Со стороны родителей в отношении системы электронных журналов важно то, что, хотя и в большой степени электронный дневник был сделан для облегчения родительского контроля за обучающимися, такой контроль при постоянном его осуществлении требует высокой мотивации родителей и наличия ряда цифровых

компетенций. Например, к одному из авторов статей обратился родитель одного из учеников с вопросом о текущей успеваемости; причиной обращения послужило то, что он увидел несовпадения оценок электронного дневника с оценками, выставленными учителем в бумажный дневник. В процессе беседы выяснилось, что учитель, заполнявший электронный журнал, по ошибке выставил неверные оценки. Такие случаи мешают родителям осуществлять качественный контроль за успеваемостью своих детей.

У части родителей отсутствует доступ в Интернет, и они требуют актуальных оценок в бумажных дневниках каждые две недели. Это требование ввиду особенностей методической работы экстраполируется на весь класс, что влечет за собой дополнительную нагрузку на педагога. Помимо мониторинга оценок, родители заинтересованы в понимании объема и содержания домашних заданий. Однако, ввиду необходимости заполнения электронного журнала в соответствии с календарно-тематическим планированием, а не «по факту», записи о домашних заданиях в электронных дневниках часто недостоверны. Нередки также случаи, когда ученики долгое время отсутствуют по причине болезни. Им следует «догнать» по успеваемости своих одноклассников и для этого они пытаются выполнить домашние задания, заданные им в течение всего срока отсутствия. Узнают эти задания они в электронных журналах и из-за этого происходит «рассинхронизация» в академическом прогрессе, ведь то, что написано в этих журналах, не соответствует действительности.

Цифровые технологии в образовательном учреждении избавит учителей от множества бумаг и пособий, так как компьютер вместит в себя множество информации, позволит более интересно и продуктивно вести урок, обучающиеся благодаря появлению цифровых технологий будут лучше ориентироваться в информационном пространстве, родители учащихся могут ежедневно проверять успеваемость по предметам, а также контролировать присутствие ребёнка в школе. Еще несомненным плюсом электронного журнала является возможность лёгкого исправления оценок или записей домашних заданий: ни для кого не секрет, что, если учитель совершил ошибку в заполнении бумажного журнала, ему придется его переписывать, так как исправлять в нём

нельзя. Однако есть и минусы: система БАРС часто «зависает», как правило это происходит под конец четверти; задания и оценки в журнале появляются несвоевременно из-за проблем интернета в школе или ввиду некомпетентности учителя. Нередки и сбои техники (проектора, компьютера) во время урока. Также после внедрения электронного журнала стало заметно пассивное ведение бумажных дневников у учащихся, а они сами должен быть ответственными за запись домашнего задания.

Контент – фильтр должен быть только на тех компьютерах, к которым у детей есть доступ: в школе это, как правило, кабинет информатики и библиотека. Для учительских ПК же должны использоваться другие правила фильтрации.

Плюсы электронного журнала такие же весомые, как и минусы, и в целом переход на цифровые и Интернет-технологии в учебном заведении должен осуществляться при условии полного оснащения техникой и организации качественной информационной инфраструктуры.

РЕГИОНАЛЬНАЯ СИСТЕМА ЭЛЕКТРОННОГО ДИСТАНЦИОННОГО ОБУЧЕНИЯ ВЛАДИМИРСКОЙ ОБЛАСТИ

Дубровина Н.Н., Мишин Д.В.

Задачи совершенствования решений связанных с электронным и дистанционным обучением (ЭДО) - повышение их производительности, устойчивости к повышенным нагрузкам, расширение функционала и т.д. для современного образования являются крайне актуальными [1]. Особенно остро эти задачи встали в связи со сложной эпидемиологической обстановкой в мире в начале 2020 года.

Как известно, процесс массового внедрения ЭДО в образовательных организациях (ОО) связан с рядом сложностей – недостаточной мотивацией и квалификацией большей части педагогов и руководителей ОО, необходимостью разработки пакета методических и административно-правовых документов ЭДО, недостатком качественного образовательного контента, необходимостью подготовки технических специалистов, способных сопровождать систему электронного дистанционного обучения (СЭДО) в ОО и т.д.. В рамках преодоления перечисленных сложностей, во Владимирской области создана и внедрена региональная система электронного и дистанционного обучения (СЭДО ВО), являющаяся модулем единой защищенной информационной среды системы образования Владимирской области. Отличительной особенностью СЭДО ВО является модульная иерархическая структура, включающая три уровня: уровень отдельной ОО, уровень муниципального образования/уровень областных организаций и региональный уровень. Так например, администратор СЭДО имеет возможность управлять сообществом/сообществами только своего уровня СЭДО ВО – администрировать учётные записи пользователей СЭДО ВО, создавать группы обучения, формировать результаты обучения, анализировать активность обучающихся, проводить экспертизу и рекомендовать курсы к публикации на вышестоящей уровень.

Такая уровневая модель позволяет СЭДО ВО решать актуальные задачи при внедрении ЭДО в ОО области, в первую очередь связанные с управлением, централизованным обновлением программно-аппаратной базы СЭДО, дистрибуцией и актуализацией образовательного контента, внедрением новых функций и т.д. Реализованные в настоящее время функции СЭДО ВО удовлетворяют большинству требований, предъявляемых пользователями – учениками, педагогами и руководителями ОО.

Кроме того, в СЭДО ВО реализована возможность рецензирования и публикации курсов на вышестоящий уровень, что является еще одной отличительной особенностью данного решения.

Для разработки учебного контента СЭДО ВО оснащена инструментами и ресурсами, позволяющие организовывать интерактивное изучение теоретического и практического материала. Например, с помощью элемента «Задание» возможно создание интерактивных упражнений, их модификация и разработка новых упражнений на основе уже созданных. Используя данный элемент, педагог, может добавить в курс такие упражнения как «найти пару», «хронологическая линейка», «кроссворд», «простой порядок», «ввод текста», «интерактивные пазлы». В процессе создания формулируются название упражнения и задание, добавляются информационные и мультимедийные объекты, подсказки и комментарии. Создание упражнений возможно для любой предметной области в рамках обобщения и систематизации знаний, а также обучающимся можно предложить в качестве домашнего задания, тем самым закрепив свои знания в игровой форме.

В элементе «Лекция» материал оформляется в виде линейной схемы, которая представляет последовательный постраничный переход, или сложной схемы, содержащей различные пути движения обучающегося. Элемент может быть использован для самостоятельного изучения темы или повторения изученного материала. Важным является то, что разработанное упражнение можно встроить в другой элемент курса, например, лекцию, обеспечив тем самым наглядность и образность подачи материала.

СЭДО ВО имеет многофункциональный тестовый элемент с возможностью формирования банка вопросов. В системе выделено несколько типов тестовых заданий: множественный выбор, альтернативный (верно/неверно), на соответствие, короткий ответ, вычисляемый. Функциональные возможности данного инструмента допускает задание шкалы, автоматическое формирование списка с оценками обучающихся и проведение анализа выполнения тестов, выставление отметок и сохранение информации о прохождении тестов обучающимися.

В СЭДО ВО реализованы средства коммуникации: форум, обратная связь, интерактивная видеоконференция, обмен личными сообщениями и файлами. Рассматривая данный блок, особое внимание стоит обратить на такой инструмент, как интерактивная видеоконференция, под которой понимается «интегрированная технология дистанционного обучения, основанная на виртуальном

взаимодействии между аудиториями слушателей, расположенных в различных территориальных и пространственно-временных границах» [2]. Базовыми функциями данного инструмента является создание вебинаров с видео – и аудиоматериалами, встроенными инструментами быстрого реагирования, виртуальной доской, загрузкой и обменом материалами, тестовым комплексом. Используя данный модуль, открывается возможность проведения онлайн-уроков в режиме живого класса.

Каждый дистанционный курс может содержать произвольное количество элементов и ресурсов, но при этом должен иметь модульный принцип. При создании структуры курса можно обращаться к ресурсу «Пояснение», который является универсальным и при продуманном использовании может улучшить внешний вид курса. Пояснение позволяет на странице портала добавлять текст и мультимедиа. Данный инструмент может использоваться для разделения длинного перечня материалов или для просмотра аудио-и видеоматериалов на странице курса, а также с целью краткого описания материала.

С целью упрощения доступа к материалам, формирования эффективного поиска, обучающимся во время обучения предоставляется доступ к библиотекам. На каждом уровне СЭДО ВО имеется публичная библиотека и библиотека сообщества. Публичная библиотека включает курсы, тематики которых являются актуальными и востребованными образовательными организациями региона. Публичная библиотека ориентирована на расширение спектра дистанционных курсов и предлагает доступ всем пользователям сообщества СЭДО ВО.

СЭДО ВО реализует обширный инструментарий для представления учебного материала, интерактивного взаимодействия между участниками образовательного процесса, организации индивидуальной и групповой учебной деятельности обучающихся, который педагог можно эффективно использовать для проведения тестирования, создания лекционных материалов, обмена информацией между пользователями или использования конкретных модулей в рамках учебных занятий. СЭДО ВО позволяет обеспечить вариативность представления информации, многократное повторение изучаемого материала, структурирование и модульность контента, выстраивание индивидуальных образовательных траекторий.

Список источников:

1. Вайндорф-Сысоева, М.Е. Методика дистанционного обучения : учебное пособие для вузов / М.Е. Вайндорф-Сысоева, Т.С. Грязнова, В.А. Шитова ; общ. ред. М.Е. Вайндорф-Сысоевой. – Москва : Юрайт, 2017. – 194 с.

2. Лупанов, В.Н. Интерактивные видеоконференции в системе открытого образования : опыт, проблемы и перспективы [Электронный ресурс] // КиберЛенинка : научная электронная библиотека. – URL: https://cutt.ly/ReAdkYS (дата обращения 18.03.2019).

3. Никуличева, Н.В. Внедрение дистанционного обучения в учебный процесс образовательной организации : практическое пособие / Н.В. Никуличева. – Москва : Федеральный институт развития образования, 2016. – 72 с.

4. Семеновских, Т.В. Методика электронного обучения / Т.В. Семеновских, С.Ф. Шляпина ; ред. В.И. Загвязинский. – Тюмень, 2015. – 56 с.

Лисина, О.В. Сравнительный анализ функциональных возможностей системы дистанционного обучения «MOODLE» в учебном процессе вуза : на примере изменений в управлении курсами «Финансовые рынки и институты» и «Экономическая теория» / О. В. Лисина, А. Н. Егоров // Экспериментальные и теоретические исследования в современной науке : сборник статей по материалам VI международной научно-практической конференции : № 6(6). – Новосибирск : СибАК, 2017. – С. 51-66.

ОБ ОПЫТЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ УЧЕНИКОВ, ОБРАБАТЫВАЕМЫХ В РЕГИОНАЛЬНЫХ АИС ОБРАЗОВАНИЯ ВЛАДИМИРСКОЙ ОБЛАСТИ

Мишин Д.В., Олейникова Е.В., Луховцова К.Д., Кондратьева А.И.

Современные информационные системы (ИС) образования предполагают, как правило, обработку не только учебно-методической, но разного рода конфиденциальной информации [1]. В первую очередь, такой конфиденциальной информацией являются персональные данные (ПДн) учащихся, их родителей и сотрудников образовательных организаций (ОО). Распределенная структура региональных ИС образования Владимирской области, обуславливают актуальность задачи разработки и реализация эффективной и безопасной цифровой образовательной среды уровня региона, позволяющей обеспечить требуемый уровень безопасности ПДн всех участников образовательного процесса.

В настоящее время на базе «Владимирского института развития образования имени Л.И. Новиковой» (ГАОУ ДПО ВО ВИРО) созданы и функционируют региональные информационные системы образования (РИСО) Владимирской области, представляющие собой комплекс интегрированных систем [2], размещенных в едином региональном центре обработки данных (РЦОД) системы образования Владимирской области. РЦОД является ядром региональной цифровой среды системы образования Владимирской области, который представляет собой информационно-технологический и программно-технический комплекс, предназначенный для организации безопасной процедуры централизованного сбора, хранения и обработки информации и оперативного предоставления различным группам пользователей доступа к информационным ресурсам, сервисам, приложениям, обеспечивающий взаимодействие между РИСО [3].

Структура РЦОД представлена серверным комплексом, хранилищем данных, системой резервного копирования данных, каналообразующим оборудованием, оборудованием защиты информации, передаваемой через публичные сети передачи данных, обеспечивающими бесперебойную работу РЦОД инженерными системами (системы гарантированного бесперебойного электропитания, системы контроля микроклимата, системы газового пожаротушения и газодымоудаления, системы контроля управления доступом в помещение и системы защиты информации, содержащейся в РИСО).

Для обеспечения защищенного доступа образовательных организаций Владимирской области (ОО ВО), муниципальных органов управления в сфере образования Владимирской области, Департамента образования (ДО) к РИСО, взаимодействия с иными защищенными сетями передачи данных (ЗСПД) и информационного взаимодействия через единое защищенное информационное пространство во Владимирской области создана (Рисунок 1) защищенная сеть передачи данных системы образования (ЗСПД СОВО).

ЗСПД СОВО предназначена для решения следующих задач:

- Информационного взаимодействия Участников ЗСПД СОВО по защищенным каналам связи;

- Защиты передаваемой информации по каналам связи ЗСПД СОВО в соответствии с требованиями законодательства РФ в области защиты сведений, содержащих ПДн и иную конфиденциальную информацию;

- Создания инфраструктуры для подключения участников ЗСПД СОВО к другим ЗСПД (ЗСПД Рособрнадзора).

Участники ЗСПД СОВО – это субъекты информационного обмена и органы, обеспечивающие данный обмен, взаимодействующие в рамках ЗСПД СОВО. К участникам ЗСПД СОВО относятся: Операторы ЗСПД СОВО; Служба сопровождения ЗСПД СОВО; Пользователи ЗСПД СОВО.

ЗСПД СОВО объединяет, сети передачи данных участников, отдельные информационные ресурсы в единую защищенную сеть с использованием различных доступных каналов передачи данных.

Все подключенные автоматизированные рабочие места (АРМ) к ЗСПД СОВО оснащены сертифицированными средствами защиты информации от несанкционированного доступа (НСД), средствами криптографической защиты информации (СКЗИ), сертифицированными средствами антивирусной защиты и аттестованы по требованиям безопасности информации [3,4]. Подключение АРМ к ЗСПД СОВО производится по одной из схем, представленных на рисунках 2-3.

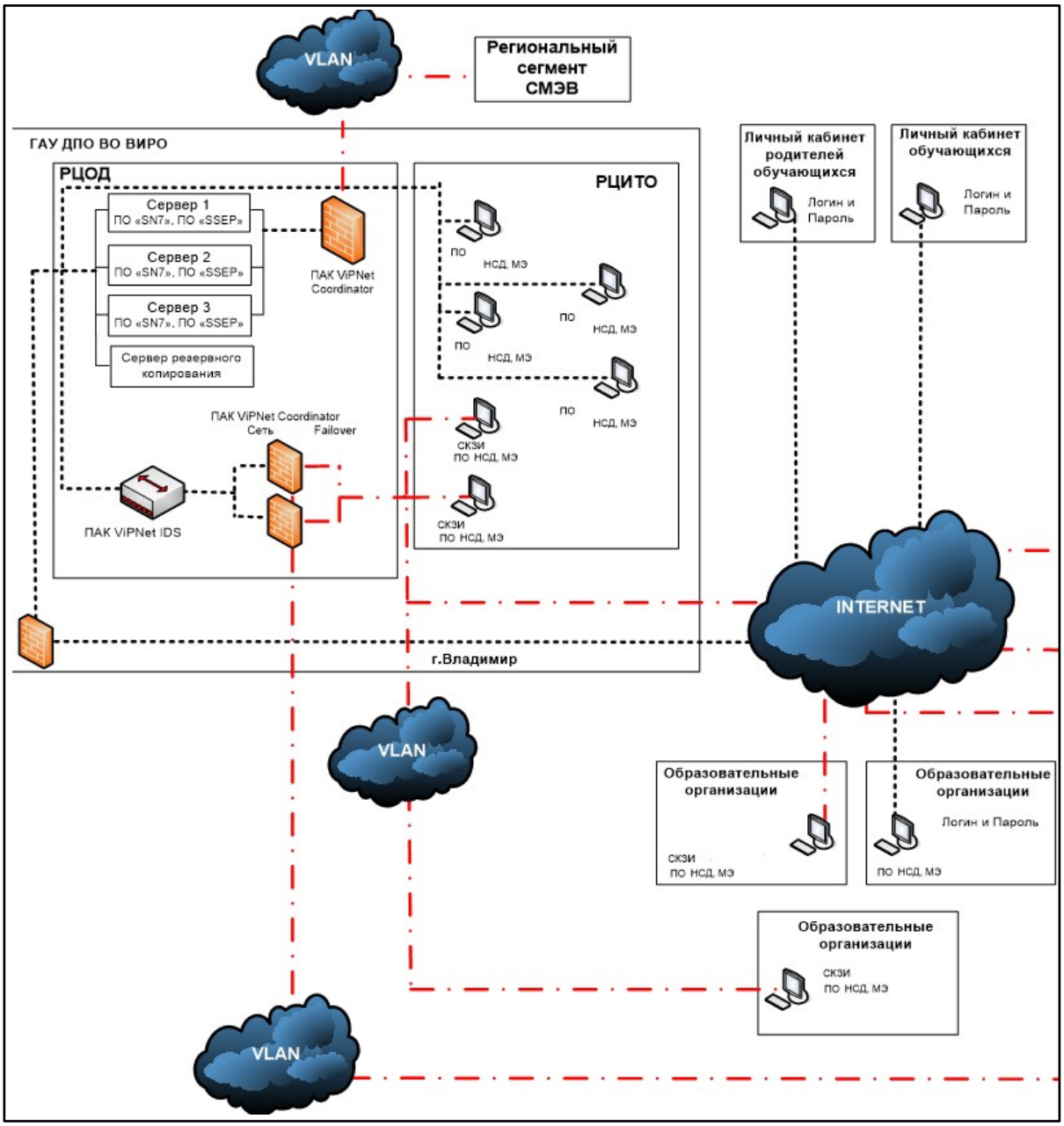


Рисунок 1 – ЗСПД СОВО

Информационная безопасность в ЗСПД СОВО обеспечивается комплексом организационных, технических мер в соответствии с требованиями регуляторов (ФСТЭК и ФСБ РФ) в области информационной безопасности [5].

Служба сопровождения ЗСПД СОВО и организации, которым поручено управление отдельными фрагментами ЗСПД СОВО, обязаны соблюдать конфиденциальность сведений, относящихся к пользователям ЗСПД СОВО, либо сведений, защищаемых в соответствии с законодательством РФ [6].

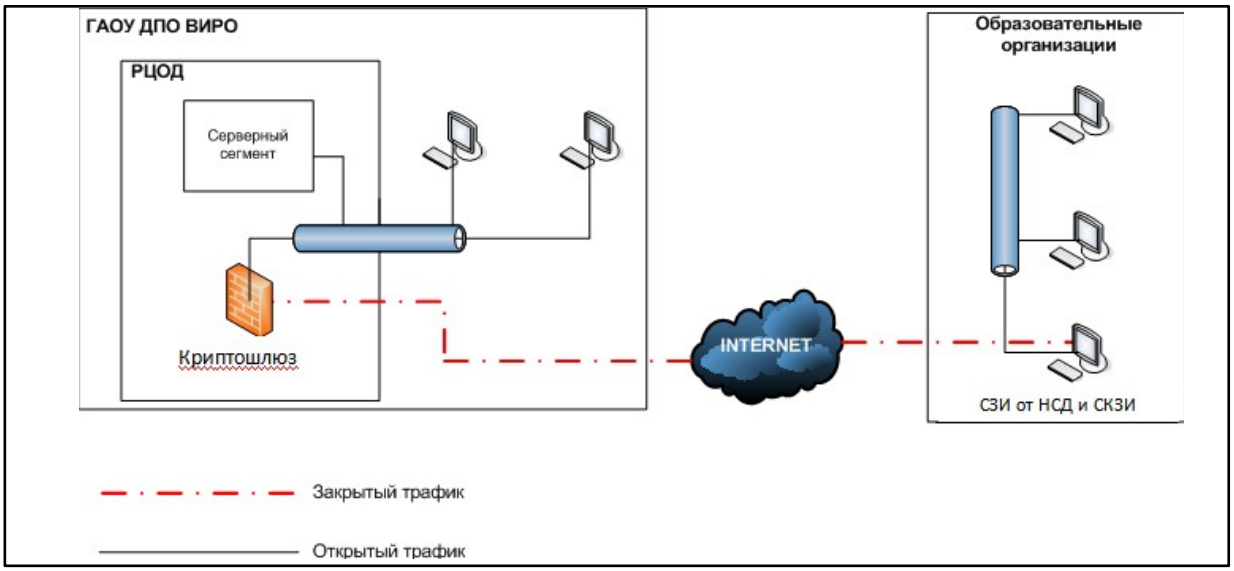


Рисунок 2 - Схема подключения при передаче данных с одного АРМ

Использование АРМ, подключенного к ЗСПД СОВО осуществляется только уполномоченными лицами пользователей и только по прямому функциональному назначению. В 2019 году ЗСПД СОВО насчитывает около тысячи пользователей.

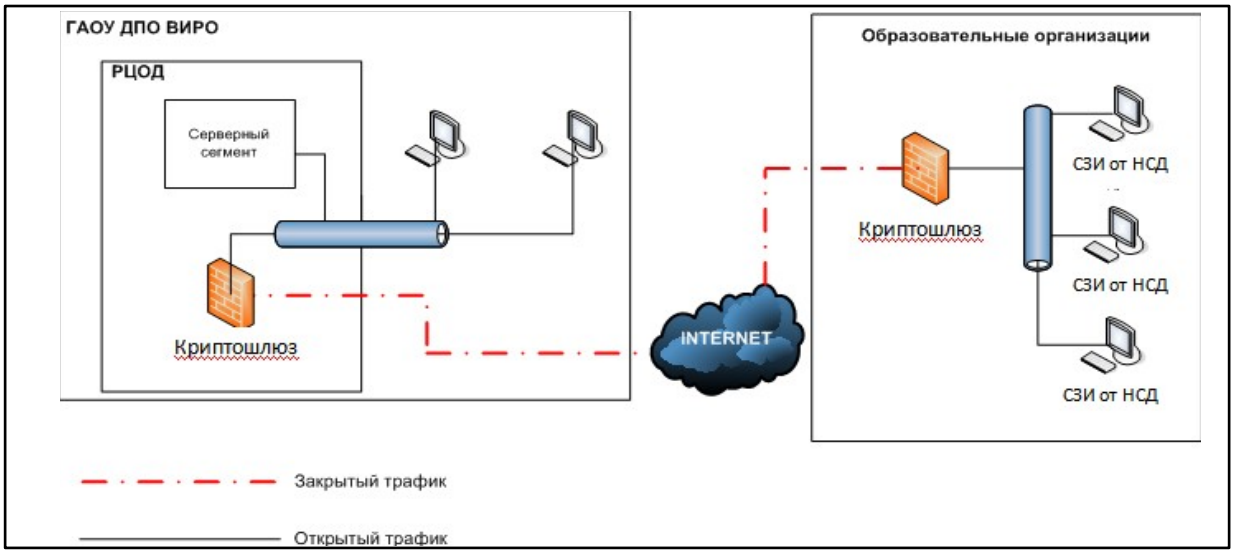


Рисунок 3 - Схема подключения при передаче данных с более 10 АРМ

Представленный в данной статье опыт построения региональной защищенной информационной среды системы образования Владимирской области показал свою эффективность, востребованность и может быть рекомендован для распространения в других регионах, в рамках решения задачи защиты персональных данных участников образовательного процесса.

Список источников:

1. Горбачев, Д.В. Общие проблемы информационной безопасности образовательного учреждения / Д.В. Горбачев, А.С. Виноградова // Интеллект. Инновации. Инвестиции. - 2014. - № 1. - С. 160-164. - ISSN: 2077-7175

2. Аспекты формирования единой информационно-коммуникационной инфраструктуры в региональной системе образования / Т.А. Орехова, И.С. Боровых, Т.Б. Белякова, Е.Н. Смирнова, Д.А. Югова // Научно-методическое обеспечение оценки качества образования / Государственное бюджетное учреждение дополнительного профессионального образования «Региональный центр оценки качества и информатизации образования». – Челябинск, [б/г]. - ISSN: 2542-0739.

3. Селифанов, В.В. Требования по защите информации при межсетевом взаимодействии государственных информационных систем с иными информационными системами / В.В. Селифанов, А.С. Гордеев, И.Н. Карманов // Интерэкспо Гео-Сибирь. - 2018. - № 7. - С. 277-282. - ISSN: 2618-981X.

4. Особенности выбора средств защиты информации в государственных информационных системах / В.В. Селифанов, С.В. Степанова, Н.А. Стрихарь, П.А. Звягинцева, Д.В. Чернов // Известия Тульского государственного университета. Технические науки. - 2018. - № 10. - С. 18-21. - ISSN: 2071-6168.

5. О выборе средств защиты информации для государственных информационных систем / А.П. Жумаева, В.А. Ялбаева, В.В. Селифанов, Д.Г. Макарова, П.А. Звягинцева, Д.В. Чернов // Известия Тульского государственного университета. Технические науки. - 2018. - № 10. - С. 52-58.

1. Труфанов, В.Н. Подход к разработке системы защиты персональных данных в государственных информационных системах / В.Н. Труфанов, С.В. Совалин, А.А. Никитин // Информатизация и связь. - 2018. - № 1. - С. 110-118. - ISSN: 2078-8320

МОДЕРНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ЗАЩИЩЕННОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ СИСТЕМЫ ОБРАЗОВАНИЯ ВЛАДИМИРСКОЙ ОБЛАСТИ

Олейникова Е.В., Мишин Д.В., Луховцова К.Д.

Для защиты конфиденциальной информации образовательных организаций во Владимирской области создана и функционирует защищенная сеть передачи данных системы образования (ЗСПД СОВО). ЗСПД СОВО объединяет, сети передачи данных субъектов информационного обмена и органы, обеспечивающие данный обмен системы образования региона, отдельные информационные ресурсы в единую защищенную сеть с использованием различных доступных каналов передачи данных. Подключение образовательных организаций (ОО) Владимирской области к ЗСПД СОВО осуществлялось поэтапно и на сегодняшний день число абонентов ЗСПД СОВО составляет более 1000. Схема сети представлена на рисунке 1.

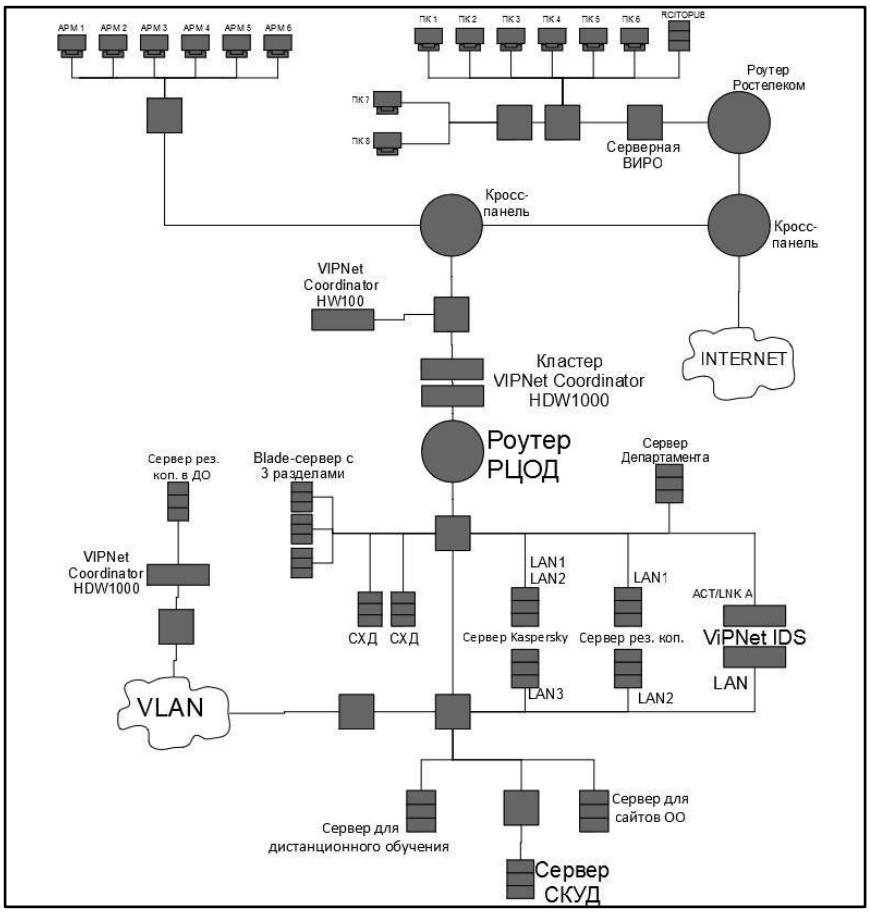


Рисунок 1. - Защищенная сеть передачи данных системы образования Владимирской области (ЗСПД СОВО).

Защита информации в ЗСПД СОВО осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области защиты персональных данных и иной конфиденциальной информации и обеспечивается комплексом организационных, технических мер в соответствии с требованиями регуляторов в области информационной безопасности (ФСТЭК и ФСБ России).

Одной из задач оператора ЗСПД СОВО является мониторинг использования средств защиты информации (СЗИ) всех абонентов защищенной сети, корректность конфигурации ЗСПД СОВО, периодичности обновления СЗИ абонентов на автоматизированных рабочих местах (АРМ) и пр. Решение данной задачи затруднено в связи со следующими особенностями объекта защиты:

- большое количество абонентов ЗСПД СОВО;
- распределенная структура ЗСПД СОВО (региональная сеть);
- компоненты ЗСПД СОВО принадлежат и управляются различным юридическим лицам;
- в образовательных организациях, отвечающих за СЗИ своих АРМ ЗСПД СОВО, как правило нет сотрудников с профильным образованием в сфере информационной безопасности.

В рамках поиска вариантов решения представленных выше задач был проведен анализ отечественных СЗИ, позволяющих осуществлять централизованное управление всеми СЗИ ЗСПД СОВО. В результате для централизованного управления СЗИ от несанкционированного доступа (НСД) в рамках реализации проекта развития системы защиты информации ЗСПД СОВО в 2019 году развернут сервер безопасности Dallas Lock 8.0-K и создан домен безопасности Dallas Lock. Для наблюдения за состоянием средств криптографической защиты информации ЗСПД СОВО, а также элементов защищенной инфраструктуры сети в 2019 году был установлен программный комплекс мониторинга защищенных сетей ViPNet StateWatcher, позволяющий осуществлять мониторинг событий безопасности и других событий, происходящих на узлах

ЗСПД СОВО, а также своевременно выявлять неполадки в работе узлов и оперативно оповещать пользователей о возникающих проблемах.

Сервер безопасности Dallas Lock 8.0-K реализован в виде службы, осуществляющей контроль за безопасностью АРМ ЗСПД СОВО. Все АРМ ОО - абоненты ЗСПД СОВО, введены под контроль сервера безопасности (стали его клиентами) и образуют домен безопасности Dallas Lock.

Программный комплекс ViPNet StateWatcher состоит из следующих компонентов:

- Сервер мониторинга — программный сервер, который выполняет следующие функции:
  - Собирает и хранит информацию о текущем состоянии узлов ЗСПД СОВО и других инфраструктурных элементов сети.
  - Выполняет анализ значений параметров состояния и формирует сообщения о выявленных событиях.
  - Оповещает операторов и администраторов системы об изменениях состояния объектов мониторинга и выявленных событиях, а также экспортирует сведения во внешние информационные системы.
- АРМ мониторинга — рабочее место администратора сервера мониторинга, позволяющее управлять одним или несколькими серверами мониторинга через защищенный канал. Доступ к данным и оповещениям о событиях сервера мониторинга осуществляется удалено через веб-интерфейс.
- Узлы мониторинга — элементы ЗСПД СОВО, состояние которых отслеживается сервером мониторинга.
- Агент мониторинга — компонент клиентского программного обеспечения ЗСПД СОВО ViPNet, которое находится на узле мониторинга и обеспечивает сбор и передачу данных о состоянии узла на сервер мониторинга.

Совместное использование рассмотренных СЗИ позволило осуществлять:

- централизованное управление пользователями и группами пользователей в ЗСПД СОВО;
- централизованное управление политиками безопасности АРМ ОО;
- централизованный просмотр и автоматический сбор журналов с АРМ ОО;
- централизованное управление доступом к ресурсам файловой системы АРМ;
- просмотр состояния отдельных клиентов ЗСПД СОВО;
- централизованный мониторинг АРМ ОО, их оборудования, определение сбоев, событий безопасности и других событий ЗСПД СОВО.
- централизованный мониторинг объектов сетевой инфраструктуры ЗСПД СОВО (маршрутизаторов, коммутаторов и т.д.), периферийного и сопутствующего оборудования (принтеры, ИБП, МФУ).

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ ЗАДАЧИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В СОВРЕМЕННОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Луховцова К.Д., Мишин Д.В., Олейникова Е.В.

В современных условиях внедрения целевой модели цифровой образовательной среды (далее – ЦОС), информационно-техническая инфраструктура образовательных организаций (далее – ОО) претерпевает значительные изменения. Одно из направлений этих изменений во Владимирской области связано с обеспечением безопасности региональных информационных систем образования («Электронная школа», «Электронный детский сад», «Электронное дополнительное образование», «Электронное и дистанционное обучение», «Мониторинговый центр», «Мониторинг образования», «Электронная библиотека», «Электронный колледж», «Информационный портал системы образования Владимирской области»). Данные автоматизированные информационные системы (далее – АИС) являются частью региональной государственной информационной системы (далее – ГИС), серверная часть которых находится в региональном центре обработки данных (далее – РЦОД), а клиенты — непосредственно в ОО области. Кроме того, в АИС обрабатываются ПДн (учеников, сотрудников организации, родителей) и обеспечение безопасности таких систем (ИСПДн, ГИС) регулируется специальными органами, так называемыми государственными регуляторами. Такими регуляторами в РФ являются ФСТЭК, ФСБ, Роскомнадзор и др.

В результате анализа основных нормативно-методических и нормативно-правовых документов регуляторов в области ИБ ГИС и ИСПДн были выявлены основные технические меры и мероприятия, которые необходимо реализовать по требованию законодательства в каждой образовательной организации для обеспечения безопасности АИС [1]:

- формирование требований к защите информации;
- разработка системы защиты информации ИС;
- внедрение системы защиты информации ИС;
- аттестация ИС

- обеспечением защиты информации в ходе эксплуатации ИС;
- обеспечение защиты информации при выводе из эксплуатации аттестованной ИС.

Рассматриваемые документы содержат требования ИБ, но не в полной мере описывают их реализацию. Авторами предлагаются следующие варианты реализации требований, адаптированные под ОО.

Требование ОО о назначении должностного лица (работника), ответственного за защиту информации может быть реализовано следующим образом:

- директор ОО назначает приказом работника ОО, ответственного за защиту информации;
- ОО разрабатывает специальную инструкцию – Должностную инструкцию ответственного за обработку ПДн и защиту информации в ОО;
- ОО может привлекать сторонние организации для обеспечения безопасности. В таком случае у сторонних организации должна быть лицензия на деятельность по технической защите конфиденциальной информации проведения некоторых работ по защите информации.

На средства защиты, которые обеспечивают защиту конфиденциальной информации в ИС ОО, накладываются требования о применении только сертифицированных средствах защиты. Сертифицированные средства защиты отличаются от несертифицированных тем, что сертифицированными являются средства, прошедшие проверку на соответствие требованиям по безопасности информации и имеющие действующий сертификат соответствия ФСТЭК и ФСБ.

На каждое сертифицированное средство защиты информации ОО должна хранить следующие документы:

- информация о сертификатах соответствия на используемое средство защиты и сроках его действия;
- сертификат соответствия в бумажном варианте;

Требования к формированию защиты информации, содержащейся в ИС ОО, включают в себя следующее:

- необходимо выявить, какие угрозы безопасности информации (далее – УБИ) возможны в ИС ОО. УБИ складываются из того, на что способен нарушитель, насколько уязвима ИС, каким образом реализуются угрозы безопасности и каковы последствия от реализации этих угроз;
- ОО должна разработать модель угроз безопасности (далее – МУ). МУ представляет собой документ, в котором описываются возможности нарушителя, уязвимости системы и последствия от нарушения свойств безопасности системы.

Для выполнения требования о разработке системы защиты информации ИС может быть выполнено следующее:

- ОО необходимо разработать техническое задание на создание системы защиты информации ИС;
- ОО разрабатывает проектную и эксплуатационную документации на систему защиты ИС;

На этапе внедрения системы защиты ОО необходимо провести анализ уязвимостей, чтобы оценить возможности нарушителя после применения системы защиты и убедиться, что УБИ предотвращены. Анализ уязвимостей должен включать в себя проверку средств защиты информации, технических средств и программного обеспечения ИС.

На этапе аттестации ИС возможны следующие варианты решения:

- ОО должна заключить договор со сторонней организацией, которая имеет право на проведение работ по защите информации, для проведения аттестации своей ИС;
- в результате аттестационных мероприятий ОО подтверждает, что их система защиты информации соответствует требованиям ФСТЭК.

По результатам аттестационных испытаний оформляются документы, перечисленные ниже:

- аттестат соответствия;
- приложение к аттестату;
- технический паспорт;
- протокол аттестационных испытаний;
- заключение (выдается по результатам проведения аттестационных испытаний);
- документ, описывающий программу и методику испытаний.

Этот перечень документов должен храниться у ОО в бумажном варианте.

Так как обязанности по обеспечению зашиты информации во время использования ИС лежат на ОО, то требования по обеспечению защиты информации в ходе эксплуатации ИС могут быть реализованы следующим образом:

- меры и мероприятия, в соответствии с которыми необходимо осуществлять защиту информации описываются в эксплуатационной документации и организационно-распорядительных документах по защите информации, составленных ОО;
- работы, которые необходимо проводить, следует проводить в течение всего времени эксплуатации ИС. Периодичность проведения таких работ определяет ОО самостоятельно и указывает период в организационно-распорядительных документах;
- одно из требований по обеспечению безопасности ИС является информирование и обучение персонала ИС ОО. Периодичность проведения практических занятий и тренировок с персоналом устанавливается ОО в организационно-распорядительных документах по защите информации, однако период проведения такого рода мероприятий не должен проходить реже одного раза в два года;
- уровень защищенности информации, содержащейся в ИС, контролируется ОО, но если ОО заключила договор по

обеспечению защиты информации со сторонней организацией, которая имеет лицензию на проведение работ по защите информации, уровень защищенности может контролировать эта сторонняя организация.

Период проведения таких мероприятий определяется ОО, однако с некоторыми ограничениями:

- в ИС 1 класса защищенности - не реже одного раза в год;
- в ИС 2 и 3 классов защищенности - не реже одного раза в два года.

При выводе из эксплуатации аттестованной ИС обеспечение защиты информации включает в себя следующее:

- если в дальнейшем ОО будет еще использовать информацию, то эта информация архивируется;
- если ОО необходимо передать машинный носитель (ремонт, техническое обслуживание), то информация стирается, если машинный носитель необходимо полностью уничтожить, то информация уничтожается.

Список источников:

1. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК от 11 февраля 2013 г. № 17.

ОБРАЗОВАТЕЛЬНЫЕ ПРОЕКТЫ ВЛАДИМИРСКОГО ИНСТИТУТА РАЗВИТИЯ ОБРАЗОВАНИЯ В ОБЛАСТИ РАЗВИТИЯ ЦИФРОВЫХ КОМПЕТЕНЦИЙ

Кондратьева А.И., Мишин Д.В.

В рамках реализации Федерального проекта «Цифровая образовательная среда», Национального проекта «Образование» школа претерпевает значительные изменения, связанные с цифровой трансформацией образования. Данный процесс связан с тем, что обучающие и обучающиеся должны получать новые знания, компетенции, повышать свои навыки, связанные с использованием цифровых знаний, цифровых инструментов. Это достаточно трудоёмкий процесс, несущий в себе определённые сложности. Владимирский институт развития образования ведёт активную работу по этим направлениям, в результате которой было решено провести серию образовательных мероприятий.

Кафедрой Цифрового образования и информационной безопасности (ЦОИБ) созданы тематические лекции и специализированные курсы, направленные на повышение цифровых и ИКТ компетенций. Материалы включают в себя элементарные и необходимые нормы не только для педагога или ученика, но и для каждого современного гражданина в XXI веке. Предусмотрены как очные, так и дистанционные курсы, так что, процесс обучения становится максимально доступным. Список курсов:

- Цифровая трансформация образования: цели, задачи, направления, инструменты.
- Современные цифровые технологии. Знакомство с Интернетом вещей (IoT)
- Современные цифровые технологии. Компьютерные сети (Networking Essentials)
- Введение в кибербезопасность (для начинающих)
- Кибербезопасность (для продвинутых)
- Основы программирования на языке Python
- Практические приемы и практики безопасной работы в сети Интернет (Основы кибергигиены)
- Цифровые риски в контексте информационной безопасности детей
- Организационно-правовые аспекты защиты информации в образовательной организации

- Организационно-технические аспекты защиты информации в ОО
- Цифровая компетентность современного учителя
- Актуальные социо-технические атаки на педагога современной школы и практики защиты от мошенничества в сети Интернет (Мошенничество в Интернет)

В качестве второго направления, в рамках сотрудничества между Координационным центром национальных доменов RU/РФ и Владимирским институтом развития образования была проведена серия образовательных мероприятий по развитию цифровых и ИКТ компетенций в форме образовательных лекций и командной интеллектуальной игры для педагогов Владимирской области. 5 школ и белее 50 педагогов приняли участие в интерактивных мероприятиях, а познакомились с некоторыми цифровыми образовательными онлайн-ресурсами. Один из них – проект **«Изучи интернет – управляй им!»**. Данный сайт включает в себя несколько вкладок, каждая из которых отлично подойдёт как для самостоятельного обучения, так и для работы с детьми.

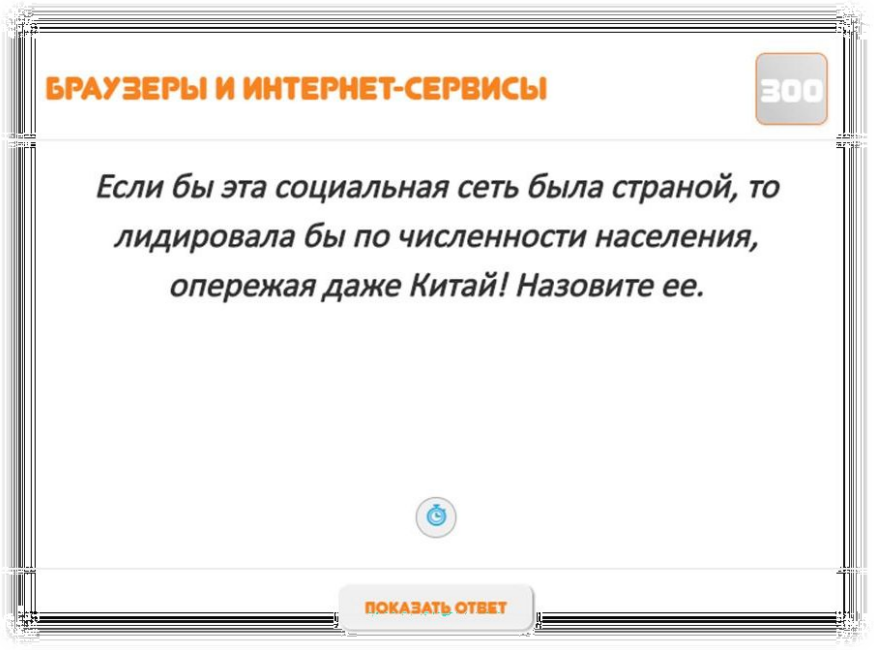
Вкладка «Тренируйся». Включает в себя несколько категорий, каждая из которых подразумевает теоретический и практический блоки. Они позволяют получать и моментально отрабатывать новые знания. Все темы имеют несколько уровней сложности, за прохождение каждого из них даются баллы. Игровой процесс затягивает не только детей, но и взрослых, а сама игровая форма покажется довольно простой и ненавязчивой. В то же время, в рамках данной вкладки затрагиваются действительно значимые темы. Так как это интернет ресурс, он не привязывает вас ни к времени, ни к конкретному месту, поэтому занятия можно проводить очно, дистанционно или изучать материал самостоятельно в любое удобное время. (Рисунки 1 и 2)

(Рисунок 1. Вкладка «Тренируйся»)

(Рисунок 2. Вкладка «Тренируйся»)

Вкладка «Викторина». Некое подобие «Своей игры». Несколько основных тем, 4 уровня сложности, возможно соревнование между 2-3 командами/участниками. Викторина постоянно развивается, пополняется новыми вопросами, новыми темами. Данная игра будет актуальна на уроке, классных часах, для соревнований между детьми, родителями, учителями или между этими категориями. Каждый участник найдёт для себя что-то познавательное. (Рисунки 2 и 4)

(Рисунок 3. Вкладка «Викторина»)



(Рисунок 4. Вкладка «Викторина»)

Кафедрой цифрового образования и информационной безопасности на базе нескольких школ области было проведено такое соревновательное мероприятие, в рамках повышения уровня цифровой грамотности и развитии цифровых и ИКТ компетенций педагогов. Данные мероприятия были оценены по достоинству и активно внедрены в учебный процесс дополнительного внеурочного образования.

Чемпионат. В 2019 году Владимирский институт развития образования принял участие во Всероссийском соревновании. Чемпионат проходил в двух категориях – «Командный зачёт» и «Индивидуальный зачёт». Множество интересных заданий, новых знаний, полезных подарков. Владимирский институт развития образования отдельно отметил участников и победителей Владимирской области. Мы искренне рады, что подобные мероприятия с каждым годом пользуются всё большей популярностью. В командном зачёте приняли участие 22 команды (более 150 участников), которые показали достойные результаты на уровне России. (Рисунок 5)

Место	Баллы	Команда
1	25900/345:9	Никологорский аграрно-промышленный колледж
2	10610/450:31	неудержимые
3	10470/190:41	Искусственный интеллект
4	6860/364:13	Искусство. Сервис. Сфера услуг
5	6650/228:55	220В
6	6530/300:16	Восхождение
7	5380/166:38	ARMY
8	5370/224:35	Брызги металла
9	5270/152:26	Девчонки
10	4930/352:2	Рожденные побеждать
11	4760/272:39	Белые шляпы
12	4410/196:49	Х@к@тон ".RU"
13	4030/253:0	Квадратура круга
14	4000/199:3	Untitled masters
15	3110/142:58	Авангард
16	2620/113:15	МБОУ "Клязьмогородецкая ООШ"
17	2220/82:6	Пятнашки
18	1690/123:30	Ардуинщики
19	1500/145:36	IT-шники
20	1290/77:10	DOMAINation
21	840/87:43	Точка роста
22	260/34:34	Медведи

(Рисунок 5. «Чемпионат»)

В заключение хотелось бы добавить, что Владимирский институт развития образования всегда открыт к сотрудничеству, в том числе и со школами. В наших и ваших интересах совместными усилиями вырастить достойное поколение, обучив их не только программам школьного курса, но и предоставив знания в таких новых областях, как кибергигиена, информационная безопасность. Поэтому особо важно уделить этим вопросам наиболее пристальное внимание, хорошо изучить самостоятельно.

ИНТЕРНЕТ РИСКИ И БЕЗОПАСНОСТЬ ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ СОВРЕМЕННОЙ ШКОЛЫ

Кондратьева А.И., Мишин Д.В.

В настоящий момент наблюдаются процессы цифровизации различных отраслей, что отражено в национальных и федеральных проектах. Серьёзные изменения уже коснулись образования, медицины, библиотечной деятельности и многих других направлений. В современной школе, в частности, в условиях самоизоляции, к обычному процессу обучения добавляется и сетевое, дистанционное. Наряду с очевидными достоинствами такой трансформации, можно говорить о появлении множества новых рисков и угроз, актуальных как для учителей, так и для детей и их родителей.

По мнению психологов, в условиях современного мира человеческий мозг испытывает колосальные перегрузки. Утренняя чашка кофе за просмотром новостей, лента в социальных сетях в течении дня, рекламы, которые постоянно борются за наше внимание, работа, домашние задания, кружки, секции… Всё сливается воедино. В условиях информационной перегруженности сложно концентрироваться на чём-то несущественном. Именно это является основной причиной роста популярности различного рода информационно-психологических атак, с применением информационно-телекоммуникационных технологий, включая интернет.

Далее рассмотрим некоторые самые популярные в атаки социальной инженерии, основная цель которых – получение различной конфиденциальной информации, паролей от социальных сетей, платёжных систем, и ПДн. Утечка ПДн может нести финансовые или коммуникационные риски, вплоть до физического контакта несовершеннолетних с незнакомыми людьми.

ФИШИНГ. С этим видом атаки, вероятно, сталкивался каждый интернет-пользователь. **Фишинг** (англ. phishing, от fishing — рыбная ловля, выуживание) — это техника интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Фишинг заключается в распространении мошеннических сообщений, вызывающих чувства срочности, любопытства, страха у человека. Такие сообщения маскируются под легальные, полученные из доверенного источника. Это самая популярная схема социальной инженерии на

сегодняшний день. Ни одна крупная утечка персональных данных не обходится без волны фишинговых рассылок, предшествующих ей.

Классическая схема фишинг-атаки:

Пользователю приходит электронное письмо или SMS-сообщение с просьбой перейти по указанной ссылке. При переходе по ссылке открывается поддельная страница известного сервиса, в точности копирующая оригинальную, где предлагается ввести логин и пароль. Не задумываясь, пользователь вводит данные, и готово – злоумышленник получает доступ к ранее защищенной информации на настоящем сайте. Да и без ввода данных, просто после открытия сайта-двойника на Ваш компьютер вполне может попасть некий «троян» непредсказуемого назначения.

Для того, чтобы понимать чему и как противостоять, важно идентифицировать эти атаки.

Для фишинга характерно:

1. Неожиданные сообщения в мессенджерах, смс, соцсетях и электронной почте от имени авторитетной организации (например, банка, платежной системы, онлайн-магазина и т.д.) С побуждением, будь то угроза или просьба, перейти по фишинговой ссылке, либо ввести информацию в прикрепленную к письму форму.

2. Баннеры и всплывающие окна, ведущие на фишинговые страницы.

3. Взломанный домен или "хороший" домен, на котором после его взлома разместили фишинговую страничку.

4. Бесплатный хостинг (зачастую фишинговая страница размещается на бесплатном хостинге).

5. Отсутствие на странице ввода конфиденциальных данных указания на то, что соединение с сайтом защищено, то есть "префикса" https:// перед адресом сайта.

6. Фишинговая страница – копия сайта организации, на клиентов которой осуществляется атака (например, банка, соцсети, платежной системы), на который перенаправляются жертвы и где они должны ввести свои конфиденциальные данные в специальные поля.

7. Фишинговый домен – доменное имя, зарегистрированное мошенниками и визуально похожее на оригинальное, но содержащее ошибки в написании.

Фишинговые сообщения могут содержать:

- сведения, вызывающие тревогу, или угрозы, например, закрытия банковских счетов, списание средств;
- запросы о пожертвованиях от лица благотворительных организаций после сообщений в новостях о стихийных бедствиях;
- грамматические и орфографические ошибки;
- обещания большой денежной выгоды с минимальными усилиями или вовсе без них;
- сведения о сделках, которые слишком хороши для того, чтобы быть правдой;

Несуществующие ссылки.

Атака, которая заключается в отправлении письма с соблазнительной причиной посетить сайт и прямой ссылкой на него, которая лишь имеет сходство с ожидаемым сайтом, например, www.PayPai.com. Выглядит это, будто это ссылка на PayPal, мало кто заметит, что буква «l» заменена на «i». Таким образом, при переходе по ссылке жертва увидит сайт, максимально идентичный ожидаемому, и при вводе данных кредитной карты эта информация сразу направляется к злоумышленнику.

Мошенничество с использованием брендов известных корпораций

В таких фишинговых схемах используются поддельные сообщения электронной почты или веб-сайты, содержащие названия крупных или известных компаний. В сообщениях может быть поздравление с победой в каком-либо конкурсе, проводимом компанией, о том, что срочно требуется изменить учётные данные или пароль. Подобные мошеннические схемы от лица службы технической поддержки также могут производиться по телефону.

Подложные лотереи

Пользователь может получить сообщения, в которых говорится о том, что он выиграл в лотерею, которая проводилась какой-либо известной компанией. Внешне эти сообщения могут выглядеть так, как будто они были отправлены от лица одного из высокопоставленных сотрудников корпорации.

IVR или телефонный фишинг

Телефонный фишинг – вишинг (англ. vishing — voice fishing) назван так по аналогии с фишингом. Данная техника основана на

использовании системы предварительно записанных голосовых сообщений с целью воссоздать «официальные звонки» банковских и других IVR систем. Обычно жертва получает запрос (чаще всего через фишинг электронной почты) связаться с банком и подтвердить или обновить какую-либо информацию. Система требует аутентификации пользователя посредством ввода PIN-кода или пароля. Поэтому, предварительно записав ключевую фразу, можно выведать всю нужную информацию. Например, любой может записать типичную команду: «Нажмите единицу, чтобы сменить пароль. Нажмите двойку, чтобы получить ответ оператора» и воспроизвести её вручную в нужный момент времени, создав впечатление работающей в данный момент системы предварительно записанных голосовых сообщений.

QUID PRO QUO

Кви про кво (от лат. *Quid pro quo* — «услуга за услугу») — в английском языке это выражение обычно используется в значении «услуга за услугу». Атака происходит тогда, когда злоумышленники запрашивают у человека личную информацию в обмен на что-то желаемое или на какой-либо вид компенсации. Очень часто такой вид атак распространяется через электронные письма, в которых требуется указать учетные данные для получения наследства, подарка, приза.

Сбор информации из открытых источников

Применение техник социальной инженерии требует не только знания психологии, но и умения просто находить необходимую информацию о человеке. Относительно новым способом получения такой информации стал её сбор из открытых источников. Подойдут активные и пассивные методы по методологии OSINT (Open source intelligence) – разведки на основе открытых источников.

К открытым источникам относятся СМИ, публикации в интернете, общедоступные данные аэросъемок и радиомониторинга, публичные отчеты государственных и коммерческих организаций, профессиональные отчеты, конференции, доклады. К примеру, такие сайты как livejournal, «Одноклассники», «ВКонтакте», содержат огромное количество данных, которые люди и не пытаются скрыть. Там можно узнать Ф. И. О. человека и его родных, телефонные номера, клички питомцев, местонахождение и запланированные поездки.

Как правило, пользователи не уделяют должного внимания вопросам безопасности, оставляя в свободном доступе данные и сведения, которые могут быть использованы злоумышленником. Даже ограничив доступ к информации на своей странице в социальной сети, пользователь не может быть точно уверен, что она никогда не попадёт в руки злоумышленников.

Предотвращение угроз Social engineering

Несмотря на применение технических средств защиты информации, данные атаки являются социальными. Поэтому единственная защита от них – просвещение. Проведение профильных семинаров, соблюдение элементарных основ цифровой безопасности при работе с интернетом (гибергигиена) для детей всех возрастов и их родителей, чтение профильно-тематической литературы, пропаганда интернет грамотности. Мы видим очевидную роль школы в решении этих задач, через создание определённых тематических кружков или секций для детей и их родителей, где в игровой форме понятной детям можно легко и ненавязчиво говорить о таких значимых и необходимых вещах. Ну и, конечно, важно помнить, что пока кибергигиене и основам информационной безопасности не будут учить в школе, пока родители не станут сами ответственно относиться к ИБ и своим примером воспитывать культуру поведения в цифровом пространстве, атаки социальной инженерии (и другие атаки ИБ) будут актуальны.

ФОРМИРОВАНИЕ НАВЫКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДСТВАМИ УЧЕБНЫХ ЗАДАНИЙ ЧЕРЕЗ ФИКСАЦИЮ ЛИЧНОСТНЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В СОСТАВЕ СОДЕРЖАНИЯ ОБРАЗОВАНИЯ

Беляева Е.А.

Актуальной задачей современной системы образования, определяемой Федеральными государственными образовательными стандартами, является формирование личностных результатов обучения школьников.

В тексте ФГОСов различных ступеней школьного образования личностные результаты трактуются как формирующаяся в образовательном процессе система ценностных отношений: обучающихся к себе, другим участникам образовательного процесса, самому образовательному процессу и его результатам, а, следовательно, достижение личностных результатов может быть надежным фундаментом для формирования критического мышления, критического отношения к информации и другим аспектам безопасного поведения детей в Сети и информационной безопасности.

Мы отмечаем, что одним из средств, где могут быть зафиксированы личностные результаты, является учебное задание, но вместе с тем в педагогическом знании и практике понимание учебного задания как средства целенаправленного достижения и фиксации личностных результатов школьников в настоящее время не нашло должного отражения.

Рассматривая учебное задание как средство фиксации личностных результатов обучения, мы основываемся на культурологической теории содержания образования В.В. Краевского – И.Я. Лернера – М.Н. Скаткина и отмечаем, что уровень учебного материала наиболее способствует формированию личностных результатов школьников.

В нашем исследовании мы рассматриваем учебное задание как педагогическое средство фиксации личностных результатов обучения на уровне учебного материала, включение которого в учебный процесс приведет к достижению личностных результатов как составляющей личностного опыта учащихся.

Обратимся к анализу подходов к их пониманию для определения педагогической сущности понятия «учебное задание».

Для нас представляет интерес точка зрения П.И. Пидкасистого, М.Д. Виноградовой, Х.Й. Лийметса, которые полагают, что задание является внешней формой самостоятельной деятельности учащихся, устанавливающая, что должен выполнить ученик, а

внутренним содержанием – познавательную или интеллектуальную задачу. Ввиду этого, учебные задания, ориентированные на достижение личностных результатов школьников мы рассматриваем как средство обогащения личностного опыта школьника в процессе учебного познания.

По мнению А.И. Умана, задание – явление, многоплановое и определить его природу в известной степени трудно. Задание может быть рассмотрено с различных позиций: а) в соотношении с содержанием образования, б) в плане деятельности; в) в плане структуры. В плане деятельности: а) задание – средство управления деятельностью ученика и контроля над ее протеканием; б) задание – ориентировочная основа деятельности и средство усвоения содержания образования.

Опираясь на позицию И.Я. Лернера, А.И. Умана, которые считают понятие «задание» наиболее общим, включающим в себя более узкие понятия – «упражнение» и «задача», термин «задание» мы будем понимать в широком смысле – как всевозможные указания интеллектуального и практического характера, направленные на организацию деятельности, осуществляемой учеником в процессе учения.

Для того, чтобы наиболее полно рассмотреть вопрос о классификации учебных заданий, необходимо обратиться к существующим различным подходам. С.Ф. Жуйков распределяет задания на две основные группы: задания, характерные для процесса приобретения знаний, умений, и задания, применяемые для закрепления изученного материала.

В нашем исследовании мы придерживаемся точки зрения А.И. Умана, который разделяет задания по такому признаку как «характер деятельности, требуемой для их выполнения». На основании этого А.И. Уман выделяет такие типы заданий как: 1) задания рецептивного характера, направленные на усвоение знаний; 2) задания репродуктивного характера, направленные на применение знаний по образцу, в знакомой ситуации; 3) задания творческого характера, направленные на применение знаний в незнакомых ситуациях.

Как видим выделены задания различного характера. Однако авторы не раскрывают особенности конструирования предложенных заданий что, на наш взгляд, создает затруднение в выделении этих способов конструирования заданий и фиксации личностных результатов обучения.

Принимая классификацию А.И. Умана, мы, в то же время, считаем возможным дополнить ее новыми классами заданий, которые сегодня становятся приоритетными в свете принятия

ФГОСов, а именно заданиями, направленными на достижение личностных результатов обучения, оставаясь в рамках предложенной системы и, используя тот же принцип, который автор положил в основу построения классификации, поскольку в ней эти задания не выделены как специальный объект.

В соответствии с представлением о качественной неоднородности личностных результатов обучения нами были выделены три основные вида учебных заданий, ориентированные на достижение личностных результатов обучения, благодаря которым возможно достижение всего спектра базовых личностных результатов обучения:

1) учебные задания, направленные на формирование готовности к самоопределению (личностному, гражданскому, профессиональному и др.);
2) учебные задания, направленные на формирование готовности к смыслообразованию;
3) учебные задания, направленные на формирование готовности к морально-этической ориентации.

Каждый вид учебных заданий конструировался таким образом, чтобы их выполнение школьниками обеспечивало достижение планируемых личностных результатов. Данный принцип определяет разнообразие учебных заданий внутри каждого вида и позволяет выделить семь основных типов учебных заданий, целенаправленно ориентированных на достижение личностных результатов обучения.

1) задания, **включающие школьников в социально-значимую творческую познавательную деятельность, имеющую культурно-созидательный характер;**
2) задания, включающие познавательную деятельность в контекст жизнедеятельности школьников;
3) задания, побуждающие школьников к социальному взаимодействию друг с другом в процессе обучения;
4) задания, направленные на формирование у школьников опыта рефлексии в познавательной деятельности;
5) задания ценностно-смысловой направленности;
6) задания, направленные на выработку у школьников критического отношения к их содержанию и формам их предъявления;
7) задания, предполагающие отсутствие границ в поиске и выборе способов выполнения учебных заданий.

Структура таких заданий может быть представлена следующим образом: первая составляющая это исторический факт либо описание жизненной ситуации, которые вызывают переживания либо «проигрывание» личностно-значимых проблем, вторая

составляющая – предметное знание и третья – вопросы для установления исторического факта/жизненной ситуации с учебным материалом (предметным знанием). Приведем примеры заданий, включающих познавательную деятельность в контекст жизнедеятельности школьников.

В содержание учебных заданий, ориентированных на достижение личностных результатов входит не только предметное знание, но и переживания учащегося, личностно значимые проблемы, описание реальных жизненных ситуаций и принятие ценностного решения в процессе выполнения задания, выбора, точки зрения, своей позиции и т.д. происходит через применение инструментов математических операций, что является основой в принятии аргументированных осознанных решений и определении своего безопасного поведения, в том числе в сети Интернет.

Список источников:

1. Асмолов, А.Г. Как проектировать универсальные учебные действия в начальной школе : от действия к мысли : пособие для учителя / ред. А.Г. Асмолова. – Москва : Просвещение, 2014. – 152 с.

2. Беляева, Е.А. Личностные результаты как планируемая цель современного школьного обучения // Вестник Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых. – 2017. – № 29(48). – С. 116-123.

3. Концепции федеральных государственных образовательных стандартов общего образования / ред. А.М. Кондакова, А.А. Кузнецова. – Москва : Просвещение, 2014. – 39 с.

1. Федеральные государственные образовательные стандарты. – URL: https://fgos.ru/ (дата обращения 10.03.2020).

ТЕРМИНАЛЬНЫЙ КОМПЬЮТЕРНЫЙ КЛАСС, КАК ВЕКТОР МОДЕРНИЗАЦИИ ИНФОРМАЦИОННО-ТЕХНИЧЕСКОЙ ИНФРАСТРУКТУРЫ ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ СОВРЕМЕННОЙ ШКОЛЫ

Аскерова А.Л., Арсенова Г.А., Волчек В.Н., Мишин Д.В.

Создание условий для внедрения современной и безопасной цифровой образовательной среды (ЦОС), обеспечивающей формирование ценности к саморазвитию и самообразованию у обучающихся образовательных организаций (ОО) всех видов и уровней, предполагает, в том числе, обновление информационно-коммуникационной инфраструктуры образовательных организаций (ОО).

Цифровая образовательная среда образовательной организации предполагает набор ИКТ-инструментов, использование которых должно носить системный порядок и удовлетворяет требованиям ФГОС к формированию условий реализации основной образовательной программы (ООП) начального общего, основного общего и среднего общего образования, способствует достижению обучающимися планируемых личностных, метапредметных, предметных результатов обучения.

Вместе с тем в практике внедрения ЦОС наблюдаются следующие противоречия:

- между современным курсом государства на импортозамещение (в том числе в ИТ-индустрии, науке и образовании) и серьезной зависимостью административно-хозяйственного и образовательного процессов в большинстве ОО (как сельских, так и городских) от импортного проприетарного (закрытого) программного обеспечения (как системного, так и прикладного);

- между динамикой развития современного цифрового оборудования, системного и прикладного программного обеспечения и циклом обновления материально-технического базы сельской школы, в том числе парка компьютерной техники и программного обеспечения;

- расширением парка цифровой техники сельской школы (в том числе в рамках программы «Точки роста»), потребностью в применении пакетов профессионального программного обеспечения в учебном процессе, навыками работы с отечественными (импортонезависимыми) операционными системами, и дефицитом

данных цифровых/ИКТ компетенций у большей части педагогов, а так же отсутствием квалифицированных технических специалистов в штате школы;

- наличием потребности в мультифункциональности компьютерного класса и применяемой цифровой техники школы, возможности адаптации конфигурации компьютерного класса под требования каждого конкретного учебного предмета или ученика и наличием в большинстве школа типового статического компьютерного класса, построенного на основе стационарных ПК и типового набора программного обеспечения.

Авторы считают, что применение технологий терминальных систем при организации компьютерного класса школы, позволит минимизировать представленные противоречия.

Во Владимирской области терминальные компьютерные классы уже применяются в двух школах – в селе Рождествено Собинского района и в селе Завалино Кольчугинского района. При этом, несмотря на то, что технология позволяет использовать наиболее популярную на сегодняшний момент ОС «Windows», в рамках поддержки отечественного производителя, а также решая задачу импортозамещения, учебный процесс был организован на отечественной ОС «АльтЛинукс».

Опыт использования терминальных классов в школе показал свою эффективность. Однако, в настоящее время терминалы организованы на основе классических персональных компьютеров, что нивелирует ряд преимуществ подхода (например, уровень электробезопасности, расхода электроэнергии, эргономики).

В настоящее время авторами ведется работа над решением следующих задач:

- анализ выработанных в условиях цифровизации образования новых моделей терминального школьного компьютерного класса (построенного на технологиях тонких клиентов);

- разработка модели терминального компьютерного класса школы, базирующиеся на технологиях *LTSP*, *X2go*, *PXE* и др., миникомпьютерной и микрокомпьютерной технике (*Raspberry Pi* и др.) и импортонезависимом программном обеспечении (*Debian GNU/Linux, ALT Linux, Rosa Linux, Debian Edu / Skolelinux Desktop* и

др.), адаптированные для преподавания предметов естественно-научного цикла;

- апробация терминального компьютерного класса, реализованного на основе разработанных моделей, доработка и оптимизация программно-технического решения в случае необходимости;

- расчет количественных показателей эффективности современного, безопасного, низко затратного, эргономичного, терминального компьютерного класса, как элемента информационно-технической инфраструктуры ЦОС современной школы;

- разработка научно-методических материалов по внедрению и техническому обслуживанию терминального компьютерного класса;

- разработка учебно-методических комплексов по предметам естественнонаучного цикла, адаптированные для проведения уроков в терминальном компьютерном классе;

- создание комплекта инструментария оценки эффективности контроля эффективности процесса обучения в условиях внедрения терминального компьютерного класса.

Решение данных задач, по мнению авторов, способствует обеспечению возможности современной школьной среде стать более безопасной, экономичной, гибкой, адаптируемой под современные требования государства и актуальные запросы учащихся.

МОДЕЛЬ ТЕРМИНАЛЬНОГО КОМПЬЮТЕРНОГО КЛАССА СОВРЕМЕННОЙ СЕЛЬСКОЙ ШКОЛЫ

Аскерова А.Л., Арсенова Г.А., Волчек В.Н., Мишин Д.В.

В рамках обеспечения реализации федерального проекта «Цифровая образовательная среда» национального проекта «Образование», в ряде сельских школ Владимирской области внедрены и функционируют компьютерные классы, построенные на технологиях терминальных систем. Опыт использования терминальных компьютерных классов в сельских школах показал свою эффективность. Однако, терминалы в настоящее время реализованы на основе классических персональных компьютеров, что нивелирует ряд преимуществ подхода (например, вопросы электробезопасности, экономии электроэнергии, эргономики, стоимости).

В работе над устранением данных недостатков, авторами была предложена своя модель терминального компьютерного класса современной школы, состоящая из комплекса организационно-методических и технических моделей: структурная модель физического пространства терминального компьютерного класса, цветовая модель физического пространства терминального компьютерного класса, аппаратно-программная модель терминального компьютерного класса.

1) **Модель физического пространства терминального компьютерного класса.**

Планируя оформления кабинета терминального компьютерного класса, за основы взяты работы: «Методика безопасного дизайна», основанная в 1971 году криминалистом Ray C Jeffery; статьи Елены Ивановой, кандидата психологических наук, доцента, заведующей лабораторией Института системных проектов МГПУ; проекты Студии дизайна образовательных пространств.

Критерии безопасной среды: естественный обзор, достаточное освещение, антивандальность, логичная структура, отсутствие тупиковых «темных» зон, чувство привязанности к помещению, его персонификация, чувство уважения к себе и защищенности, территориальность.

Структурная модель физического пространства терминального компьютерного класса современной школы предполагает разделение среды класса на три пространственные зоны:

- Зона трансляции знаний (стена, на которой расположена школьная доска и телевизор).

- Зона для работы с учебным материалом (3 ряда по 3 парты).

- Зона инноваций (разборный шестигранный стол, состоящий из модулей столов-трапеций, на которых размещены рабочие места обучающихся, оборудованные терминалами).

Шестигранная конфигурация стола зоны инноваций дает возможность группе обучающихся работать, как над решением одной задачи в коллективе, так и индивидуально над своей определенной исследовательской проблемой.

Цветовая модель физического пространства терминального компьютерного класса современной школы.

При разработке цветовой модели терминального компьютерного класса был введен свой цветовой акцент для каждой пространственной зоны. Цветовое решение должно добавить пространству терминального компьютерного класса более явную структуру, позитивное настроение и зонировать функциональные области.

Базовый цвет стен открытый, светлый бежевый. Стены класса оформляются следующим образом:

- Стена с окнами напротив двери, покрашены в 2 цвета бежевый и белый в пропорции 2/3 и 1/3. Жалюзи имеют бежевый цвет.

- Стена с доской не нагружена цветом.

- Стена напротив доски и стена напротив окон - цветами обозначены функциональные зоны: в которых размещаем разные обучающие материалы и интерактивные поверхности.

Пол покрыт коммерческим линолеумом и имеет нейтральный серый цвет.

Модель физического пространства компьютерного класса предполагает создание эргономичной - удобной, комфортной и здоровье сберегающей среды в терминальном компьютерном классе современной школы.

2) Аппаратно-программная модель терминального компьютерного класса современной школы.

Решение основано на использовании в качестве рабочих мест обучающихся (АРМ) терминальных компьютеров (функционирующих по технологии тонких клиентов), подключенных через локальную сеть к терминальному серверу.

Терминалы (тонкие клиенты) – бездисковые компактные персональные компьютеры (оборудованные периферийными устройствами — клавиатура, мышь, монитор, акустические системы и т. д.) не имеющие собственных вычислительных мощностей.

Решение всех вычислительных задач, связанных с работой прикладных приложений, необходимых школьникам в рамках учебного процесса, ложиться на терминальный сервер.

Терминальный сервер компьютерного класса (1 шт.):

- Процессор CPU Intel Core i5-7400 3GHz/4core/SVGA HD Graphics 630/1+6Mb/65W/8 GT/s LGA1151, Мат.платаASRock H110M-HDV R3.0 (RTL) LGA1151<H110> PCI-E Dsub+DVI+HDMI GbLAN SATA MicroATX 2DDR4, Модуль памяти Kingston <KVR24N17S8/8> DDR4 DIMM 8Gb <PC4-19200> CL17, Накопитель SSD 250 Gb SATA 6Gb/s SanDisk Ultra 3D <SDSSDH3-250G-G25> 2.5.

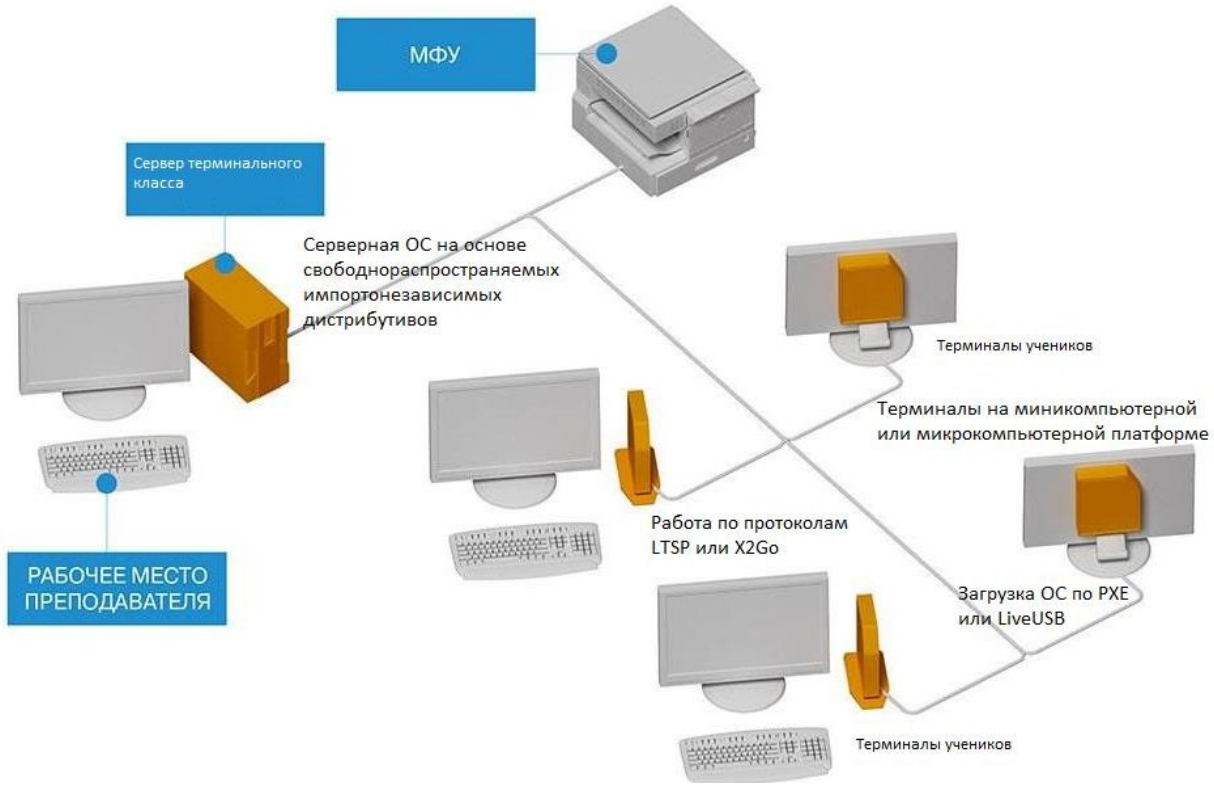
- ОС на базе современных дистрибутивов *Linux* (*ALT, Debian, Rosa, Ubuntu*), ltsp-server-standalone, x2goserver, x2goclient, Virtual Box.

Функции: централизованное управление терминалами, предоставление среды для выполнения пользовательских приложений, необходимых в рамках учебного процесса, мониторинг и корректировка деятельности учеников и организация механизмов для предоставление оперативной помощи.

Терминалы тип 1 (5 шт.): Платформа GIGABYTE GB-BACE-3160 (Celeron J3160, 1.6-2.24 ГГц, SVGA, HDMI, GbLAN, WiFi, BT,SATA.1DDR3 SODIMM);

Терминалы тип 2 (2 шт): ПЭВМRaspberry PI3 model B+ (1.4GHz, 1Gb, HDMI, GbLAN, WiFi, BT. 4xUSB, microSD, 40xGPIO).

Функции: обеспечение интерфейса взаимодействия ученика и пользовательских приложений, необходимых в рамках учебного процесса.



Ожидаемые эффекты внедрения терминального компьютерного класса современной школы на основе данной модели

1. Повышение уровня цифровых/ИКТ компетенций как учеников, так и педагогических работников.
2. Повышение эффективности деятельности учителя посредством снижения временных затрат на вспомогательные процессы.
3. Снижение временных затрат на обслуживание компьютерного класса;
4. Снижение финансовых затрат на обслуживание и модернизацию компьютерного класса;
5. Снижение уровня шума в компьютерном классе;
6. Снижение уровня энергопотребления компьютерного класса;
7. Повышение уровня электробезопасности учеников.

АЛГОРИТМЫ ВНЕДРЕНИЯ ТЕРМИНАЛЬНОГО КОМПЬЮТЕРНОГО КЛАССА В СОВРЕМЕННОЙ ШКОЛЕ

Черешнев М.Н., Волчек В.Н., Мишин Д.В.

Постепенно системы, основанные на использовании толстых и тонких клиентов, проникают в различные сферы жизни современного человека. Не обошли своим присутствием тонкие клиенты и сферу образования, где в учебных классах школьники и студенты решают однотипные специализированные задачи, которые, как правило, не требуют больших ресурсов персональных компьютеров.

Так, в школах по всему миру стали внедряться решения на базе тонких клиентов, и тому есть несколько причин: расширение возможностей компьютерных вычислений, обогащение средств контроля для преподавателей и системных администраторов, повышение заинтересованности учащихся и сокращение общих затрат на управление и обслуживание компьютерных сетей в образовательных учреждениях.

В общем виде система терминального класса является классическим примером взаимодействия толстого и тонкого клиентов. В качестве толстого клиента в компьютерном классе выступает сервер, к которому по локальной сети подключены машины, не имеющие операционных систем - тонкие клиенты.

Программное обеспечение для создание такой инфраструктуры рассматривается следующее: в качестве операционной системы сервера – любой Debian - подобный дистрибутив Linux, программное обеспечение для удаленного доступа – X2go или Ltsp.

X2Go – это программное обеспечение с открытым исходным кодом, для удаленного администрирования машин Linux которые используют протокол NX technology. **X2Go** дает удаленный доступ к графическому интерфейсу Linux. Защищенность соединения предоставляется благодаря использованию ssh. Серверный пакет должен быть установлен на машине с Linux. Клиентские приложения для доступа к серверному хосту могут быть запущены на любой машине

Linux Terminal Server Project (LTSP) — это свободно распространяемый дополнительный пакет для Linux с открытым исходным кодом, который позволяет нескольким людям с маломощными компьютерами (терминалами) использовать вычислительные мощности одного более производительного

компьютера (сервера). При этом, все приложения запускаются на сервере, а терминалы, так же называемые тонкими клиентами (или X-терминалами), просто принимают видеоряд, посылаемый сервером, и кроме него ничего не обрабатывают. Как правило, терминал представляет собой маломощный компьютер, в нём даже может отсутствовать жесткий диск, вследствие чего он может работать тише, чем обычный настольный компьютер.

Примечание: можно использовать обе эти технологии на одном сервере, они отлично совместимы.

Установка и конфигурирование LTSP:

1. Выбор способа загрузки по сети

Клиентская система после включения питания должна получить IP-адрес вызвав DHCP-запрос, путь к загружаемому ядру и путь к каталогу который будет использован вместо корневого. Есть несколько вариантов, позволяющих сделать это, необходимо лишь выбрать более подходящий ситуации: сетевая загрузка, используя Etherboot, PXE, MBA, Netboot, не говоря уже о том, что можно просто загрузиться с дискеты, CD-ROM, USB или выбрав нужный пункт в меню при загрузке с жесткого диска.

2. Установка сервера LTSP

LTSP доступен как набор пакетов для установки на Linux-системе, последние версии легко интегрируются в Ubuntu, Debian, Fedora Core, Gentoo и некоторыми другими дистрибутивами.

1) Проверить наличие ltsp в пакетном менеджере.
2) Установить следующие пакеты: ltsp-server-standalone и openssh-server (DHCP сервер идет в составе первого пакета).
3) Установить пакет ltsp-utils, он включает в себя две утилиты для упрощения настройки и администрирования ltsp. Это ltspadmin и ltspcfg.
4) Создание рабочего окружения клиентов утилитой ltsp-build-client.
5) Настройка сервисов NFS и DHCP, на этом этапе задается пул адресов для клиентов, настраивается DNS и остальные конфигурации сети.
6) Настройка TFTP
7) Перезагрузка всех используемых серверов.

Установка и конфигурирование X2Go:

1. Установка ядра сервера X2Go

1) Добавление официального репозитория X2Go в систему.
2) Установка основных пакетов ядра: x2goserver и x2goserver-xsession.
3) Настройка сессий.
4) Настройка сети.

2. Построение системы тонкого клиента (Среда Chroot)

1) Установка пакета x2gothinclientmanagement, основной компонент системы тонких клиентов.
2) Настройка файла конфигурации x2gothinclient_settings.
3) Создание новой среды chroot для тонкого клиента.
4) Перенос конфигураций для сессий на pxe-сервер.
5) Обновление настроек.
6) Конфигурация DHCPD.
7) Конфигурация общего ресурса NFS.
8) Конфигурация x2go client в режиме диспетчера отображений.
9) Перезагрузка всех сетевых сервисов.

В одной из школ Владимирской области будет внедрен терминальный класс по предложенным алгоритмам установки и конфигурации систем, основанных на программном обеспечении X2Go и LTSP.

ИМИТАЦИОННАЯ МОДЕЛЬ ПРИОРИТИЗАЦИИ ТРАФИКА НА ОСНОВЕ АЛГОРИТМА HTB В СЕТЯХ TCP/IP

Бедняцкий И.С.

Приложения и сервисы можно «грубо» разделить по чувствительности к задержкам на два класса: асинхронные и синхронные. К асинхронным относятся те приложения, которые нечувствительны к задержкам передачи данных в очень широком диапазоне, вплоть до нескольких секунд, а все остальные приложения, на функциональность которых задержки влияют существенно, относят к синхронным приложениям. [3]

Использование алгоритмов приоритизации трафика позволяет отделять синхронный трафик и выделить ему гарантированную полосу пропускания. Таким образом, на данный момент разработка алгоритмов приоритизации трафика является актуальной задачей.

Token Bucket. Алгоритм ведра маркеров (Token Bucket) используется для сглаживания и профилирования трафика. Он основан на сравнение потока пакетов с эталоном потоком.

Token Bucket состоит из двух буферов – для пакетов и жетонов (tokens) (Рисунок 1). Эталонный поток представлен жетонами, заполняющими условное “ведро” (буфер) жетонов.

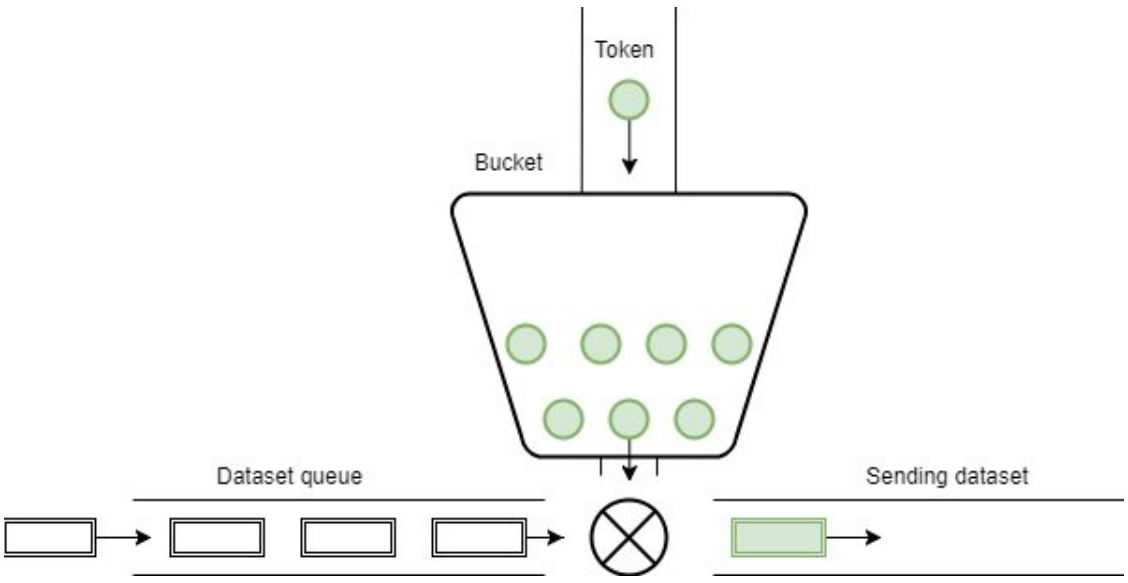


Рис. 1 - Схема алгоритма Token Bucket

Под жетонами (маркерами) в данном случае понимается некий абстрактный объект. Пакет проходит только в том случае, если в ведре достаточно для него жетонов. Жетоны, используемые прошедшим пакетом, удаляются из буфера.

Hierarchical Token Bucket (HTB). Данный алгоритм подразумевает разделение полосы пропускания для определенных потоков в отдельные классы, каждый из которых имеет свою собственную полосу пропускания. Классы могут разделяться на дочерние классы, каждый из которых будет делить между собой полосу родительского класса. Каждый класс соответствует определенному типу трафика и имеет свой приоритет. Пакеты приходят на обработку только в листовые классы (очереди). [2]

Дерево алгоритма строится из дочерних и родительских классов. Класс называется корневым, если он является непосредственным потомком дисциплины HTB. Родительские классы могут предоставлять часть своего канала соседним классам, но сами заимствовать каналы не могут.

Если привести аналогию с алгоритмом Token Bucket, то в данном случае под выделенной полосой пропускания класса подразумеваются токены класса, которые он использует. Когда классу недостаточно полосы пропускания, он пытается подняться выше по дереву, получив таким образом больше токенов.

Модернизация HTB. Главной разницей смоделированной системы от оригинального алгоритма является то, что при распределении полосы пропускания планировщик руководствуется соблюдением максимального директивного времени для высокоприоритетного трафика. В то время оригинальный алгоритм смотрит на загруженность очередей в классах.

Если задержка класса больше установленного директивного времени, то он будет пытаться подниматься вверх по дереву алгоритма, заимствовав больше полосы пропускания до тех пор, пока задержка не станет удовлетворительной. В случае, когда текущая задержка класса гораздо меньше заявленного директивного времени, класс будет отдавать заимствованную им полосу пропускания, если такая имеется. [1]

Моделирование алгоритма. Имитация описанной модели производилась в среде моделирования AnyLogic.

Схема модели изображена на Рисунке 2, где листьями являются очереди, изображенные в виде прямоугольника. Круг A представляет из себя корневой класс A, а круг B промежуточный класс B, потомок первого и третьего листа. Сами пакеты приходят на обработку только в листья.

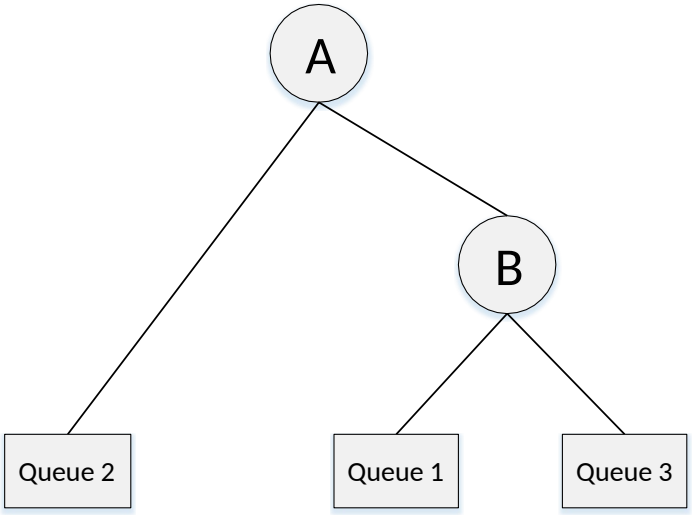


Рис. 2 - Схема моделируемой системы

Для первой очереди максимальной задержкой, при которой не нарушается работа приложения, являются 2 мс, для второй – 5 мс, для третей – 10 мс.

Тестирование. Для определения эффективности проведем смоделированной модели проведем тестирование с различными способами генерации трафика.

В первом тесте класс трафика с наивысшим приоритетом генерируется в соответствии с нормальным распределением, а два класса меньшего приоритета распределением Парето.

Таблица 1 – Результаты первого тестирования

Класс приоритета	Значения	Средние значения
Класс 1	Количество пакетов на входе	9943
	Пакеты не прошедшие за мдв (%)	6,50
	Средняя задержка	0,96
Класс 2	Количество пакетов на входе	4649
	Пакеты не прошедшие за мдв (%)	5,82
	Средняя задержка	1,67

Класс 3	Количество пакетов на входе	2994
	Пакеты не прошедшие за мдв (%)	18,32
	Средняя задержка	7,06

Во втором тесте трафик генерируется также, как и в первом, но к каждому классу прибавлена переменная изменяющаяся во времени. Значение переменной максимально в начале и конце эксперимента, минимально в середине.

Таблица 2 – Результаты второго тестирования

Класс приоритета	Значения	Средние значения
Класс 1	Количество пакетов на входе	9653
	Пакеты не прошедшие за мдв (%)	4,16
	Средняя задержка	0,86
Класс 2	Количество пакетов на входе	4242
	Пакеты не прошедшие за мдв (%)	4,81
	Средняя задержка	1,51
Класс 3	Количество пакетов на входе	2926
	Пакеты не прошедшие за мдв (%)	13,61
	Средняя задержка	6,31

В третьем тесте класс трафика с наивысшим приоритетом генерируется в соответствии с нормальным распределением, класс меньшего приоритета распределением Парето, а оставшийся класс трафика генерируется в соответствие с определенным периодом.

Таблица 3 – Результаты третьего тестирования

Класс приоритета	Значения	Средние значения
Класс 1	Количество пакетов на входе	10025
	Пакеты не прошедшие за мдв (%)	5,83
	Средняя задержка	0,95
Класс 2	Количество пакетов на входе	4550
	Пакеты не прошедшие за мдв (%)	17,49
	Средняя задержка	3,29
Класс 3	Количество пакетов на входе	3113
	Пакеты не прошедшие за мдв (%)	24,80
	Средняя задержка	8,07

Заключение. В ходе работы была разработана имитационная модель приоритизации трафика в программном обсечение для моделирования AnyLogic, основным отличием которой от исходного алгоритма приоритизации является планирование очередей передачи данных в зависимости от соблюдение допустимых задержек для разных типов трафика.

На основе проведенного тестирования можно сказать что модель справляется с задачей распределения количества обрабатываемых пакетов по приоритету и при максимальной нагрузке количество пакетов, не проходящих за максимальное директивное время, в классах высокого приоритета не превышает 7%.

МОДЕРНИЗИРОВАННЫЙ АЛГОРИТМ HTB В СЕТЯХ TCP/IP

Ниязов Р.Х., Монахов Ю.М., Бедняцкий И.С., Балашов В.И.

В статье представлен краткий анализ предметной области, подход к повышению доступности узлов автоматизированных систем и модифицированный алгоритм на базе ОС Linux. Так же было проведено тестирование данного алгоритма в модернизированной конфигурации.

Введение. Задержка — важный фактор, обеспечивающий надёжную работу и высокую производительность сетей. При достижении оптимальной задержки будут без проблем функционировать сервисы для общения в реальном времени, стриминга и проведения транзакций.

Внедрение алгоритмов приоритизации, позволяет обеспечивать доступность трафика чувствительного к задержкам канала.

Предметом исследования являются модель и программный комплекс, основанный на алгоритме контроля задержек при обслуживании комплекса для приоритизации задержек, а также управления QoS (качеством обслуживания).

Анализ предметной области. QoS уже зарекомендовала себя как технология, обеспечивающая конвергенцию голосовых, видеосетей и сетей передачи данных. По мере развития потребностей бизнеса растут и требования к технологиям QoS.

Обеспечение достаточного качества обслуживания в IP-сетях становится все более важным аспектом современной корпоративной ИТ-инфраструктуры. QoS не только имеет важное значение для передачи голоса и видео по сети, но и является важным фактором поддержки развивающегося Интернет-вещей.

Алгоритм HTB. В результате анализа предметной области можно сделать вывод, что для обеспечения должных откликов сервисов, применяют метод приоритизации трафика посредством классификации трафика. Чаще всего для классификации трафика используется алгоритм планирования Hierarchical Token Bucket.

Классовая дисциплина HTB предназначена для разделения полосы пропускания между различными типами трафика, каждый из которых может получить выгоду от гарантированной полосы пропускания. В настоящее время HTB широко используется для реализации эффективных и многоуровневых систем управления трафиком.

Модифицированный HTB. Для повышения качества обслуживания были внесены следующие модификации в алгоритм:

- Контроль значения задержки очереди;
- Динамическое изменении задержки очереди передачи канала относительно входящей интенсивности;
- Контроль переполнения буфера.

Тестовое сравнение результатов на моделях. (Таблица 1) В тестировании принимали участие две модели: первая модель, где избыток токенов класса отдавался листу с самым высоким приоритетом, и вторая модель, где избыток токенов делился между листовыми классами по формуле. Далее представлены режимы тестирования. Каждый тест проводился 2 минуты, и отмечалась задержка для каждого пакета.

Режим тестирования	Интенсивность очереди 1 (пакет/мс)	Интенсивность очереди 2 (пакет/мс)	Интенсивность очереди 3 (пакет/мс)
Режим 1	5	5	50
Режим 2	50	50	5
Режим 3	50	5	50
Режим 4	5	50	50
Режим 5	50	50	50
Режим 6	40	40	40

Таблица 1 Параметры тестирования

В данном режиме тестирования заметно, что вторая модель (Рис. 2) проявляет себя хуже, чем первая модель (Рис. 1). Это связанно с тем, что для удовлетворения задержки второй очереди необходим весь избыток класса A, но так как первая очередь почти всегда использует свою часть избытка A, то для второго класса наблюдаются лишние потери, которые отсутствуют в первой модели.

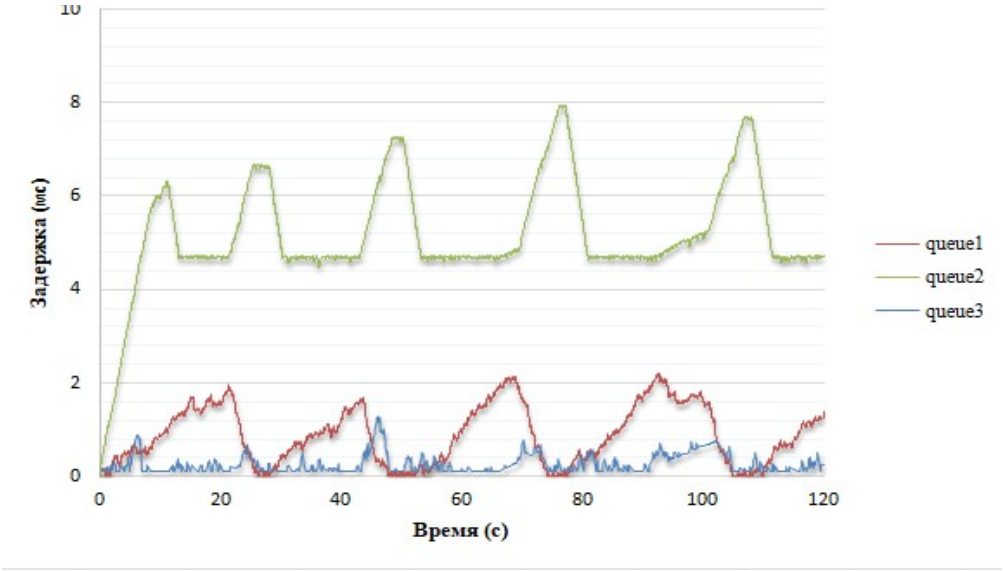


Рис. 1 Результат тестирования модели 1 в режиме 2

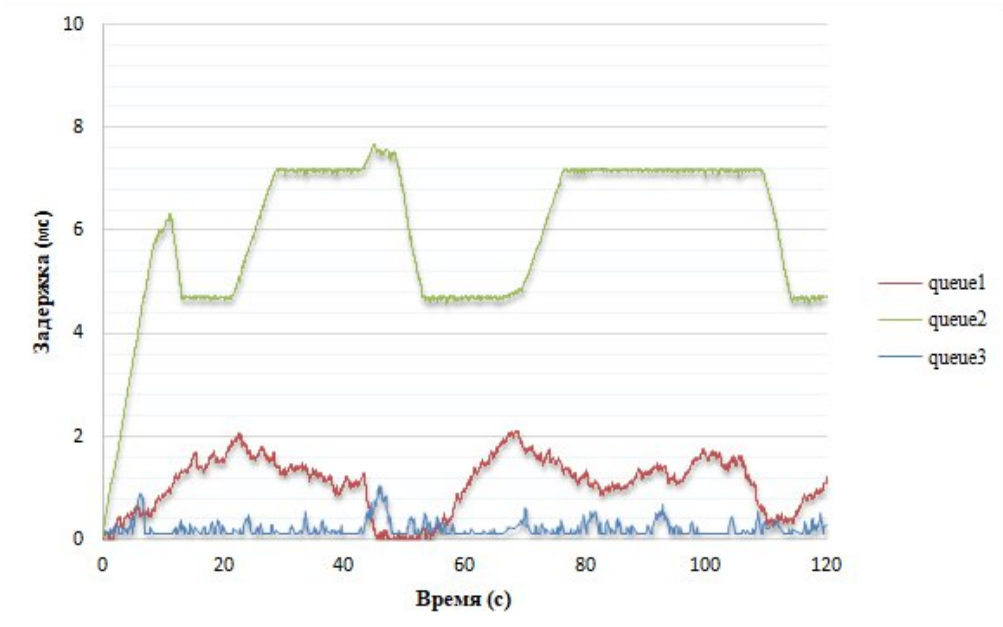


Рис. 2 Результат тестирования модели 2 в режиме 2

В данном режиме тестирования лучшие результаты показывает первая модель (Рис. 3). Вторая модель (Рис. 4) имеет такие же проблемы, как и во втором режиме тестирования: второй очереди недостаточно зарезервированных токенов.

В пятом режиме тестирования модели показали разные результаты. Во второй модели (Рис. 6), в отличие от первой (Рис. 5), сократились потери для третей очереди по сравнению с первой, однако были потеряны почти все пакеты второй очереди.

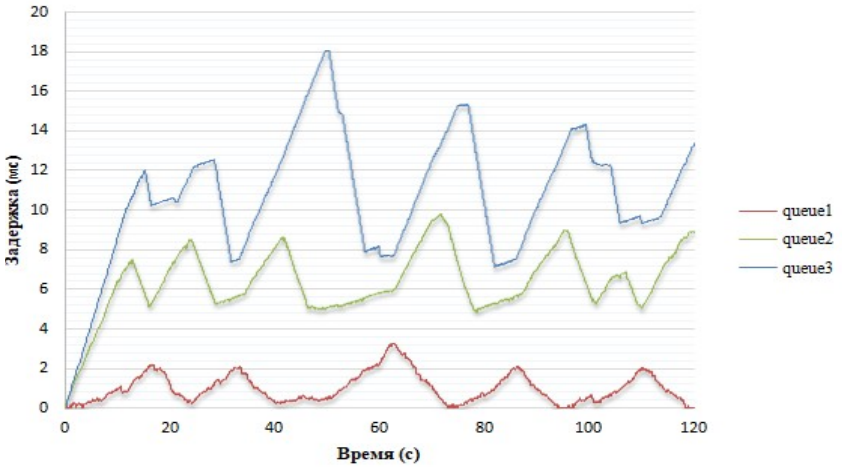


Рис. 3 Результат тестирования модели 1 в режиме 4

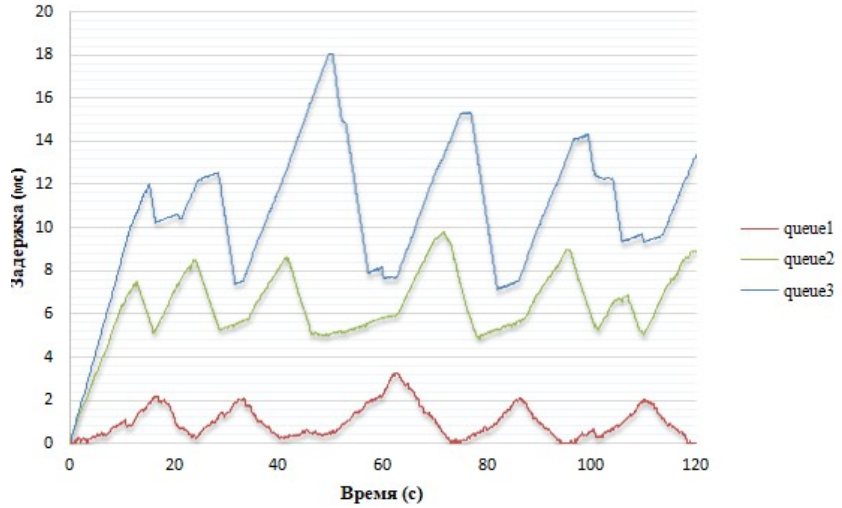


Рис. 4 Результат тестирования модели 2 в режиме 4

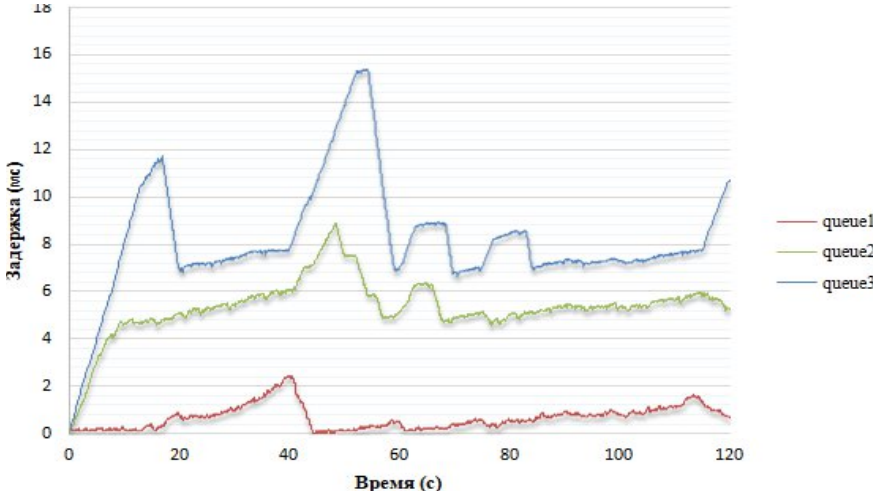


Рис. 5 Результат тестирования модели 1 в режиме 5

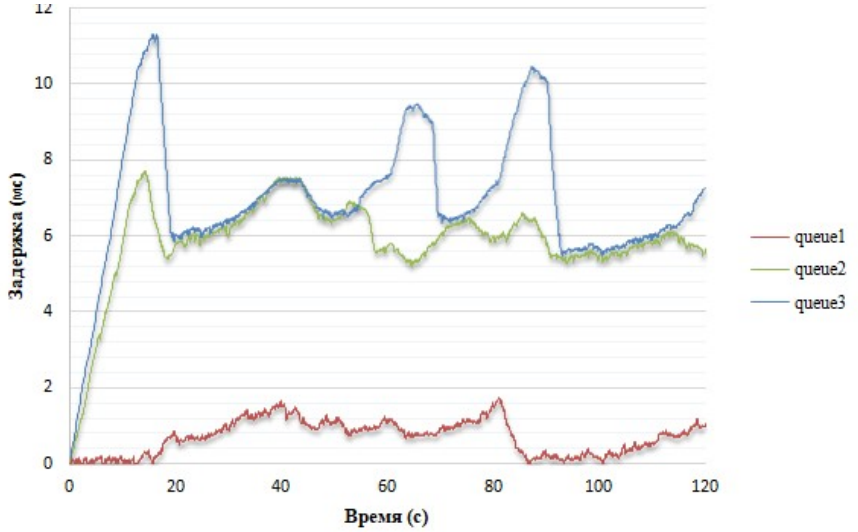


Рис. 6 Результат тестирования модели 2 в режиме 5

Вывод. Модель плохо проявляет себя, когда классу необходимо количество токенов, намного превышающих количество гарантированных токенов для класса. Однако в том случае, когда количество необходимо токенов классу не сильно превышает количество гарантированных токенов или класс имеет много родителей, у которых зарезервированы для него токены, данная модель показывает более стабильную задержку для класса.

Список литературы

1. Доработка имитационной модели алгоритмов приоритизации в сетях TCP/IP / Р.Х. Ниязов, Ю.М. Монахов, И.С. Бедняцкий, В.И. Балашов, А.П. Кузнецова // Девятая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности. – 2019. – С. 479–485.

2. Monakhov, Yu.M. Prioritization To Ensure Availability in Telecommunication Networks of Textile Enterprises / Yu.M. Monakhov, A.P. Kuznetsova, A.V. Pestov // Известия высших учебных заведений. Технология текстильной промышленности. – 2018. – С. 159-163.

1. Дисциплина обработки очереди HTB. Руководство по использованию [Электронный ресурс] 2006 г. / Алексей Ремизов // OpenNet. - URL: https://www.opennet.ru/base/net/h tb_manual.txt.html (Дата обращения 15.08.2019)

АНАЛИЗ УСТОЙЧИВОСТИ АЛГОРИТМОВ УПРАВЛЕНИЯ ПЕРЕГРУЗКАМИ В ВИРТУАЛЬНОМ КАНАЛЕ TCP/IP

Романченко С.С., Монахов Ю.М.

Протокол управления передачей (Transmission Control Protocol, TCP) широко используется в современных сетях. Алгоритм случайного раннего обнаружения (Random Early Detection, RED) в настоящее время является наиболее перспективным и обсуждаемым алгоритмом повышения производительности TCP. Модель системы TCP/RED состоит из двух взаимодействующих между собой частей: очереди, которая получает поток пакетов и реагирует на изменения интенсивности, и TCP-источников, каждый из которых реагирует на потерю пакета в очереди (что определено механизмом контроля потока TCP). В данной работе будет использоваться упрощенная версия алгоритма RED, которая выглядит следующим образом (1).

$$\begin{cases} \dfrac{d\bar{s}}{dt} = \bar{\lambda}\left(t - \dfrac{R}{2}\right)\beta\left(\bar{q}(t) - \bar{s}(t)\right), \\ \dfrac{d\bar{q}}{dt} = \bar{\lambda}\left(t - \dfrac{R}{2}\right)\left(1 - \pi^{k}\right)\left(1 - p(\bar{s}(t))\right) - \mu(1 - \pi^{0}), \\ \dfrac{d\bar{\lambda}}{dt} = -\dfrac{P_L(t - \frac{R}{2})}{2m}\bar{\lambda}(t - R)\bar{\lambda}(t) + (1 - P_L(t - \frac{R}{2}))\dfrac{m}{R^2}\dfrac{\bar{\lambda}(t - R)}{\bar{\lambda}(t)}. \end{cases} \quad (1)$$

С помощью $\bar{s}(t)$ обозначена усредненная длина очереди, $\bar{q}(t)$ – мгновенная длина очереди, $\bar{\lambda}(t)$ – средняя скорость прибытия пакетов.

Запишем $\bar{q}(t)$, зависящую от λ(t), с помощью формулы Полячека-Хинчина:

$$\bar{q}(\lambda) = \lambda + \frac{\lambda^2}{2(1-\lambda)}(1 + C^2) \quad (2)$$

Где C^2 - дисперсия распределения длины пакета. Следовательно, наша модель RFDE становится:

$$\frac{d\bar{s}}{dt} = \bar{\lambda}\left(t - \frac{R}{2}\right)\beta\left(\bar{q}\left((1 - p(\bar{s}(t)))\,\bar{\lambda}\left(t - \frac{R}{2}\right)\right) - \bar{s}(t)\right),$$

$$\frac{d\lambda}{dt} = -\frac{p\left(\bar{s}\left(t-\frac{R}{2}\right)\right)^2}{2m}\lambda(t-R)\lambda(t) + \left(1-p\left(\bar{s}\left(t-\frac{R}{2}\right)\right)\right)R^2\frac{\frac{m\,\bar{\lambda}(t-R)}{R}}{\bar{\lambda}(t)}. \quad (3)$$

С помощью полученной формулы построим графики, описывающие поведение системы.

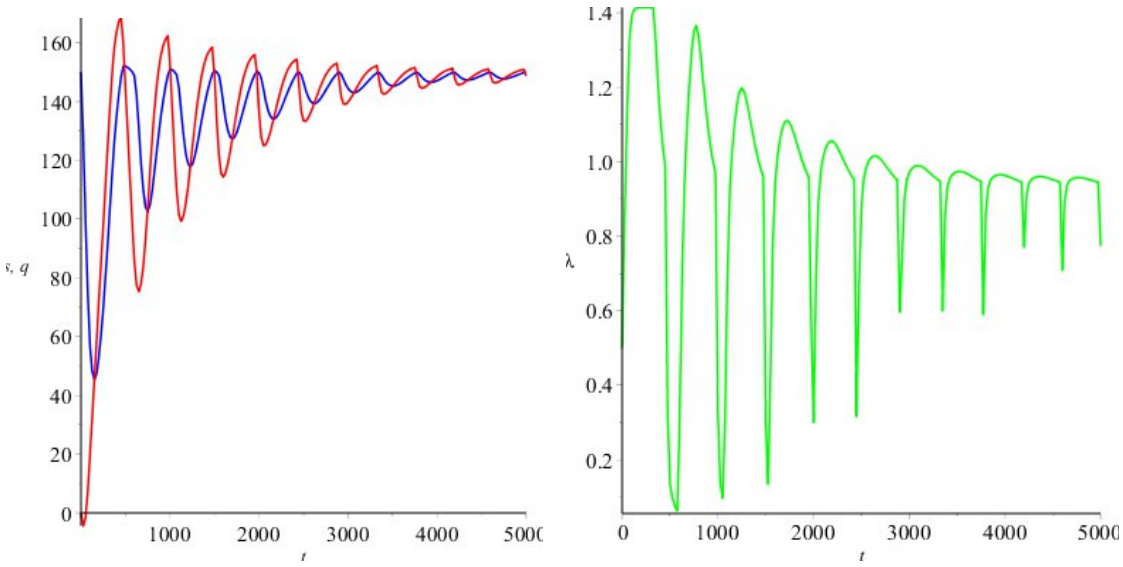


Рис. 1

Графики (рис. 1) показывают зависимость функций средней длины очереди, мгновенной очереди(слева) и интенсивности подачи пакетов в очередь(справа) от времени. В случае проведения ряда экспериментов, можно заметить, что стабильность системы определяют 3 параметра: R, m и μ. Подстраивая их так, чтобы система стала стабильной, можно проследить зависимость между этими 3 переменными (рис. 2).

$$R \sim km \qquad (4)$$

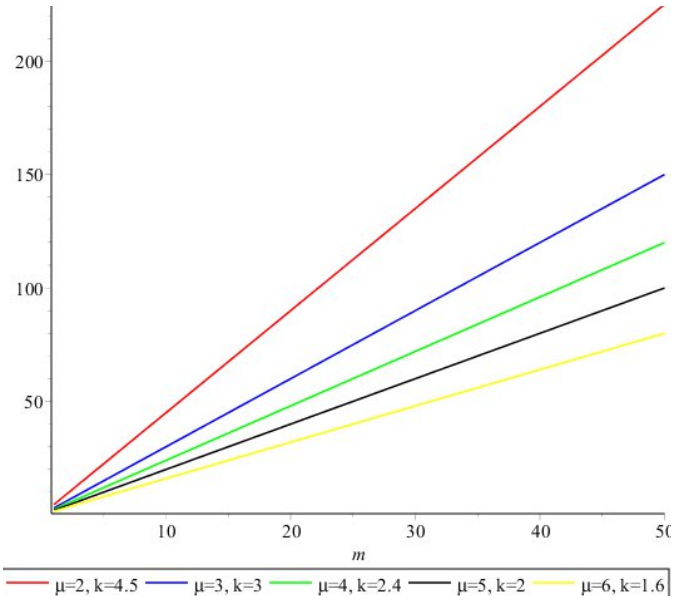


Рис. 2

На графике видно, что чем меньше интенсивность обслуживания заявки, тем больше коэффициент k и время задержки для одного и того же количества источников.

При линеаризации уравнения удалось вывести следующую формулу:

$$\begin{cases} a_0 = \dfrac{e^{Rx}y(a_2^2+2a_2x+x^2-y^2)}{\gamma(x,y)} \\ a_1 = -\dfrac{(a_2+2x)y\cos(Ry)+(a_2x+x^2-y^2)\sin(Ry)}{\gamma(x,y)} \end{cases} \quad (5)$$

где $\gamma(x,y) = y\cos(Ry) + (x + a_2)\sin(Ry)$.

Удалось вывести лемму, которая указывает на существование точек равновесия, где достигается стабильность системы.

Лемма

При определенных условиях существуют области решений z* характеристического уравнения линеаризованной динамической системы, для которых выполняются условия устойчивости $a_1 \geq 0$, $a_0 \geq 0$, и существуют точки равновесия (s*, λ*) = φ(z* ϵ Z*), находящихся в области допустимых состояний уравнения.

$$\exists\, z \in Z;\ z = x + iy:\ a_1 \geq 0,\ a_0 \geq 0 \quad => \quad (6)$$

$$\exists\, Z^* \subset Z:\ \forall\ \ z^* \in Z^*\ \exists(s^*, \lambda^*) = \varphi(z^*)$$

Проделанная работа заключается в анализе предметной области, и требует дальнейшего решения в виде поиска точек равновесия для данной системы.

МАШИННО-СИНЕСТЕТИЧЕСКИЙ ПОДХОД К ОБНАРУЖЕНИЮ СЕТЕВЫХ АТАК ТИПА DDOS

Яшнов И.В., Монахов Ю.М., Маков Е.О.

Введение. Distributed Denial of Service или «Распределенный отказ от обслуживания» — нападение на информационную систему для того, чтобы та не имела возможности обрабатывать пользовательские запросы. Простыми словами, DDoS заключается в подавлении веб-ресурса или сервера трафиком из огромного количества источников, что делает его недоступным. Соответственно, возможность распознать атаку типа DDoS является одной из составляющих решения проблемы доступности ресурса.

Методы обеспечения доступности. Одним из методов обеспечения доступности сети является использование механизмов обнаружения сетевых аномалий. Прежде чем определить аномалию, необходимо выяснить, что считается нормальным состоянием. Мы рассматриваем состояние системы как «нормальное» (или «функционально жизнеспособное»), когда оно выполняет все назначенные ей функции.

Следовательно, аномалия — это состояние, при котором поведение системы не соответствует четко установленным характеристикам нормального поведения.

DDoS атака рассматривается как аномалия, которую необходимо обнаружить.

Машинная синестезия. При своевременном обнаружении аномалий повышаются шансы на своевременное и эффективное реагирование на атаки на нарушение доступности сети. Методы машинной синестезии в данном случае понимается представление в виде изображения и последующий анализ набора параметров, которыми представлена модель сети и проходящий через неё трафик. Данные методы в сочетании с методами машинного зрения потенциально имеют важный набор преимуществ над классическими методами: высокая скорость реагирования на аномалию и низкие требования к вычислительным ресурсам.

Так же в основе данного метода лежат сети адаптивной критики.

Сеть адаптивной критики. В представленной модели используется принцип обучения через взаимодействие с окружающей средой, в таком случае к стандартной модели обучения с подкреплением вида< S, A, R, T, γ > где:

S – конечный набор состояний;

A – конечный набор действий;

R: $S \times A \times S \rightarrow \mathbb{R}$ - функция награды;

T: $S \times A \rightarrow \Delta S$ – вероятность перехода;

$\gamma \in [0, 1]$ – фактор дисконтирования;

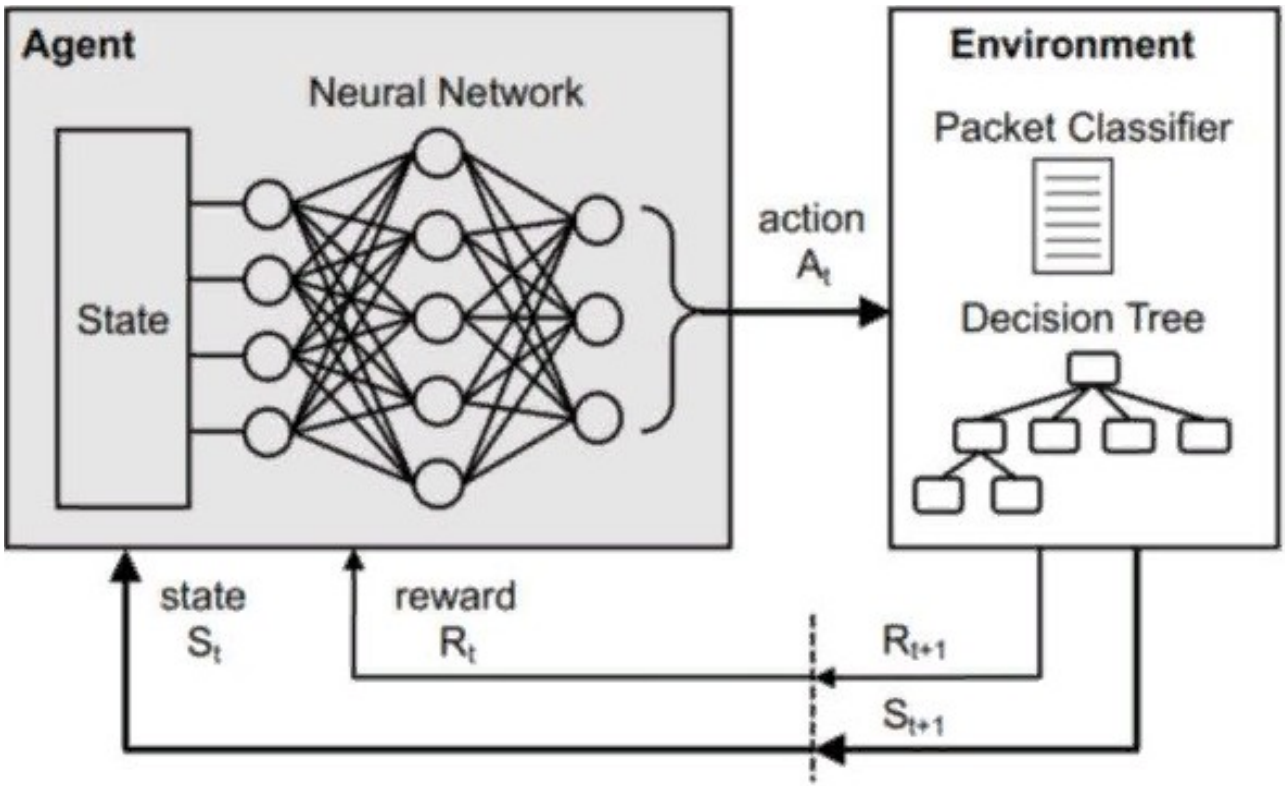


Рисунок 1 – Модель сети с адаптивной критикой.

- Среда (Environment) – предобученный классификатор, метрики которого мы хотим повысить;
- Агент (Agent) – нейронная сеть, которая предсказывает вектор значений;
- Событие (Action) - вектор базиса, который используется для проекции точек многомерного пространства;
- Состояние (State) – состояние среды в момент времени t (изображение по новым пакетам сетевого трафика);
- Вознаграждение (Reward) – разница между предсказанным и реальным значением класса.

Начальный подход к предлагаемой модели. Извлечение информативных признаков из сетевого дампа – сначала отбираются нужные параметры траффика с которыми будем работать, все параметры собираются в один многомерный вектор

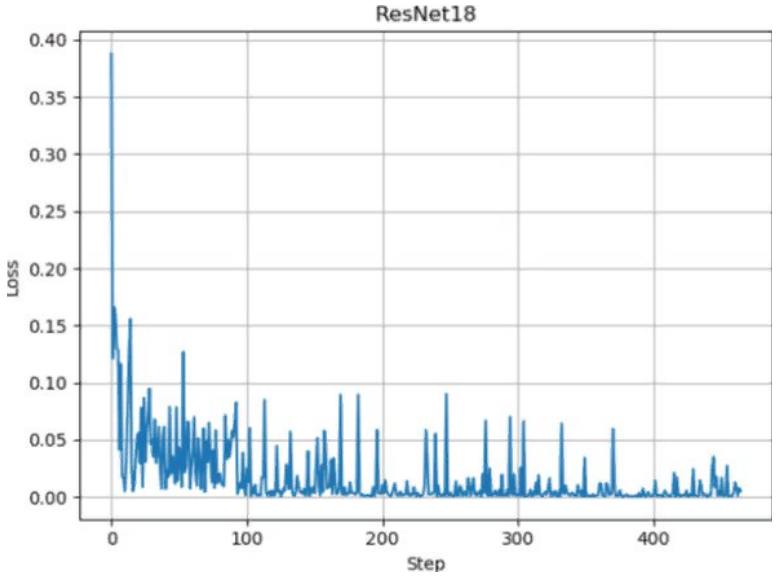
Преобразование признаков векторов в точки 4-ех мерного пространства (RGBA - RGBA расшифровывается как Red Green Blue Alpha. На W3C объясняется: «В этой спецификации цветовая модель RGB расширена и включает составляющую альфа, позволяющую задать непрозрачность цвета» Это значит, что можно добавить четвертое значение (от 1 до 0), чтобы задать уровень непрозрачности данного RGB-цвета.);

Благодаря цветовой модели RGBA можно полученные точки 4х-мерного пространства преобразовать в изображения.

После форматирования данных необходимо обучить классификатор, в качестве алгоритма репрезентации данных в изображение был использован алгоритм используемый в статье A Machine-Synesthetic Approach To DDoS Network Attack Detection Полученные изображения в формате RGBA, используются для обучения классификатора.

Результаты обучения классификатора. По результатам, представленным ниже, получили классификатор высокой точности (90%).

Далее планируется использовать полученный классификатор для интегрирования в описанную выше модель.



Вывод. В ходе вышеописанной работы был получен классификатор высокой точности, в дальнейшем его необходимо интегрировать в систему адаптивной критики.

Список литературы

1. Список литературы

1. A Machine-Synesthetic Approach To DDoS Network Attack Detection [3.1 Image representation of multidimensional TCP/IP traffic data https://arxiv.org/pdf/1901.04017.pdf].

РЕЗОЛЮЦИЯ

Резолюция
VIII Межрегиональной конференции «Диалог-online»
«Актуальные вопросы безопасности
в глобальной информационной среде»

27 февраля 2020 года

Участники VIII Межрегиональной конференции «Диалог-online» «Актуальные вопросы безопасности в глобальной информационной среде», поддержанной государственной программой Владимирской области «Обеспечение информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции во Владимирской области на 2014 – 2020 годы».

отмечают:

Вопросы безопасности в глобальной информационной среде на сегодняшний день являются одними из наиболее важных для современного общества.

Как взрослые, так и дети активно пользуются современными цифровыми технологиями в режиме 24/7 для решения самых разным задач, однако правила безопасного и ответственного использования данных технологий знакомы далеко не всем.

Цель родителей, образовательных организаций, библиотек и других институтов образования и воспитания детей – научиться самим и научить ребенка эффективно, этично и безопасно использовать возможности современных цифровых технологий (в том числе, Интернета), повысить общий уровень цифровой компетентности и цифровой культуры нашего общества.

Вопрос этот особенно актуален в связи с Десятилетием детства, объявленным в соответствии с Указом Президента РФ от 29 мая 2017 года. Он требует уделять детям и молодежи самое пристальное внимание, стремиться к тому, чтобы они могли научиться думать, самостоятельно принимать решения, достигать новых высот.

Добиться этого можно только совместными усилиями органов и учреждений культуры, образования, общественности.

С целью решения актуальных вопросов безопасности в глобальной информационной среде

рекомендуется:

1. Усилить координацию и взаимодействие межведомственных структур по созданию безопасной информационной среды.

2. Принять эффективные меры по созданию привлекательного для детей и молодежи позитивного онлайн-контента.

3. Государственному бюджетному учреждению культуры Владимирской области «Владимирская областная библиотека для детей и молодежи» выступить в качестве региональной площадки проведения всероссийского диктанта по киберграмотности для школьников средних классов.

4. Развивать сотрудничество с Академией инновационного образования и развития, Национальной родительской ассоциацией по вопросам внедрения во Владимирской области новых форм просветительской работы по продвижению безопасного интернета.

5. В воспитательной работе обратить особое внимание на выстраивание конструктивного диалога между школой, родителями и детьми.

6. Учить молодежь работать с информацией с учетом понятий негативного контента, фейковой информации, постправды.

7. Принять меры по внедрению контент фильтров в местах с общедоступным доступом в Интернет

8. Уделить внимание развитию фондов библиотек, регулярно пополнять их качественными и актуальными изданиями, связанными с вопросами кибербезопасности, кибергигиены, цифровой грамотности, безопасности детей в Интернет и т.д.

9. Создать банк позитивных практик по информационной безопасности на площадках Владимирского института развития образования имени Л.И. Новиковой, Владимирской областной библиотеки для детей и молодежи.

10. Активнее подключать к решению вопросов создания безопасной информационной среды цифровых волонтеров, в том числе из числа студентов Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых.

АЛФАВИТНЫЙ УКАЗАТЕЛЬ АВТОРОВ

Волчек Виктор Николаевич,

стр.67, 70, 74.

Федеральный исследовательский центр "Информатика и управление" Российской Академии Наук, инженер-исследователь.

Дубровина Нина Николаевна,

стр.35.

Государственное автономное образовательное учреждение дополнительного профессионального образования Владимирской области «Владимирский институт развития образования имени Л.И. Новиковой», методист РЦИТО.

Зубанова Екатерина Андреевна,

стр.30

Муниципальное бюджетное образовательное учреждение «Рождественская средняя общеобразовательная школа» Собинского района, заместитель директора по воспитательной работе.

Кондратьева Алёна Игоревна,

стр.39, 53, 58.

Государственное автономное образовательное учреждение дополнительного профессионального образования Владимирской области «Владимирский институт развития образования имени Л.И. Новиковой», лаборант кафедры ЦОИБ.

Луховцова Кристина Дмитриевна,

стр.39, 44, 48.

Государственное автономное образовательное учреждение дополнительного профессионального образования Владимирской области «Владимирский институт развития образования имени Л.И. Новиковой», ведущий программист РЦИТО.

Маков Евгений Олегович,

стр.89.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых», студент каф. ИЗИ.

Мишин Денис Вячеславович, к.т.н.,

стр.35, 39, 44, 48, 53, 58, 67, 70, 74.

Государственное автономное образовательное учреждение дополнительного профессионального образования Владимирской области «Владимирский институт развития образования имени Л.И. Новиковой», заведующий кафедрой ЦОИБ.

Монахов Юрий Михайлович, к.т.н.,

стр.30, 82, 86, 89.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых», доцент кафедры ИЗИ.

Некрасова Светлана Владимировна,

стр.20.

Государственное учреждение культуры «Донецкая республиканская библиотека для молодежи», главный библиотекарь отдела социокультурной деятельности.

Ниязов Рустам Хайруллович,

стр.82.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых», студент каф. ИЗИ.

Новикова Татьяна Ивановна,

стр.27.

Координационный центр доменов .RU/.РФ, руководитель социальных проектов.

Олейникова Екатерина Владимировна,

стр.39, 44, 48.

Государственное автономное образовательное учреждение дополнительного профессионального образования Владимирской области «Владимирский институт развития образования имени Л.И. Новиковой», руководитель РЦИТО.

Научное издание

ДИАЛОГ-ONLINE

Материалы VIII межрегиональной конференции
27 февраля 2020 года

Ответственный за выпуск: Сдобникова Т.А.
Ответственный редактор: Мишин Д.В.
Макет, компьютерная вёрстка: Кондратьева А.И.

Бумага для офисной полиграфии 80 г/кв.м. Объём 6,25 усл.п.л.
Формат 60×90 см, 1/16 доля.
Подписано в печать *******. Заказ №****
Тираж 100 экз.

Отпечатано в типографии ГАОУ ДПО ВО ВИРО имени Л.И.Новиковой