Департамент культуры администрации Владимирской области
Государственное бюджетное учреждение культуры Владимирской области
«Владимирская областная библиотека для детей и молодежи»
Департамент образования администрации Владимирской области
Государственное автономное образовательное учреждение дополнительного
профессионального образования Владимирской области
«Владимирский институт развития образования имени Л.И. Новиковой»
при участии
Кафедры информатики и защиты информации
Государственного бюджетного образовательного учреждения высшего профессионального
образования
«Владимирский государственный университет имени Александра Григорьевича и Николая
Григорьевича Столетовых»

ДИАЛОГ-ONLINE

Сборник материалов VI Межрегиональной
научно-практической конференции
26 февраля 2018 г.

Владимир
2018

Департамент культуры администрации Владимирской области

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

Департамент образования администрации Владимирской области

Государственное автономное образовательное учреждение дополнительного
профессионального образования Владимирской области
«Владимирский институт развития образования имени Л.И. Новиковой»
при участии
Кафедры информатики и защиты информации
Государственного бюджетного образовательного учреждения высшего профессионального
образования
«Владимирский государственный университет имени Александра Григорьевича и Николая
Григорьевича Столетовых»

Диалог-online

Сборник материалов
VI Межрегиональной научно-практической
конференции
в рамках Государственной программы
«Обеспечение информационной безопасности детей,
производства информационной продукции для детей
и оборота информационной продукции
во Владимирской области на 2016-2018гг.»

26 февраля 2018 года

Владимир
2018

ББК 78.38

Д 44

Составитель: Артемьева К.Ю., ведущий методист отдела инновационно-методической работы;

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

Диалог-online: сборник материалов VI Межрегиональной научно-практической конференции в рамках Государственной программы «Обеспечение информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции во Владимирской области на 2016-2018гг.», 26 февраля 2018 года / Департамент культуры администрации Владимирской области; Департамент образования администрации Владимирской области; Владимирская областная библиотека для детей и молодежи; Владимирский институт образования им. Л.И. Новиковой; Владимирский государственный университет им. А.Г. и Н.Г. Столетовых. – Владимир, 2018. – 54с.

В докладах участников Конференции всестороннее рассмотрение получили такие проблемы, как: технологии проведения ctf- соревнований во Владимирской области, оптимальные родительские стратегии регуляции использования детьми видеоигр, информационное противодействие негативным тенденциям в процессе формирования глобального информационного общества, особенности защиты информационной среды общеобразовательных организаций Владимирской области, влияние современных инфокоммуникационных технологий на образ жизни, воспитание и личностное становление подрастающего поколения.

Материалы сборника публикуются с сохранением авторского стиля.

Введение

Сборник составлен по итогам VI Межрегиональной научно-практической конференции «Диалог-online», состоявшейся 26 февраля 2018 года.

Межрегиональная конференция «Диалог-online» организуется и проходит на протяжении 5 лет, освещая наиболее актуальные вопросы, связанные с интернет-безопасностью и работой в сети Интернет. Сборник включает в себя 10 докладов.

Конференция проходит в рамках Государственной программы «Обеспечение информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции во Владимирской области на 2016-2018 гг.».

Шестая по счету встреча состоялась на базе «Детского технопарка «Кванториум»», при активной поддержке представителей данного центра, администрации Владимирской области и Главного управления Центрального банка РФ по Центральному федеральному округу.

Делая краткие выводы по прошедшей конференции, можно отметить ее актуальность и общественную значимость. Многие из участников поддержали идею привлечения к данной теме не только специалистов соответствующих сфер, но и приглашение глав родительского комитета, учителей и других, чья деятельность связана с подрастающим поколением и применением инновационных технологий.

Во встрече приняло участие более 90 человек, среди которых были эксперты отдела безопасности и защиты информации отделения по Владимирской области Главного управления Центрального банка Российской Федерации по Центральному федеральному округу, сотрудники Международной сетевой академии CISCO, аспиранты Института психологии Российской Академии Наук, инженеры-исследователи Института Проблем Информатики Российской Академии Наук, кандидаты технических наук, доценты, студенты кафедры информатики и защиты информации Владимирского государственного университета им. А.Г. и Н.Г. Столетовых.

На конференции были рассмотрены такие вопросы как: технологии проведения ctf- соревнований во Владимирской области, оптимальные родительские стратегии регуляции использования детьми видеоигр, информационное противодействие негативным тенденциям в процессе формирования глобального информационного общества, особенности защиты информационной среды общеобразовательных организаций Владимирской области, влияние современных инфокоммуникационных технологий на образ жизни, воспитание и личностное становление подрастающего поколения, проблемы взаимоотношений между родителями и детьми в эпоху глобального распространения сети Интернет.

В данном сборнике представлены 10 докладов участников конференции. Порядок размещения – хронологический, в соответствии с выступлениями докладчиков.

Монахов Ю.М., Порфирьев А.А., Шеремет Д.А., Харламов А.Р., Татова Е.Д.,

г. Владимир

ТЕХНОЛОГИИ ПРОВЕДЕНИЯ CTF- СОРЕВНОВАНИЙ ВО ВЛАДИМИРСКОЙ ОБЛАСТИ

Во Владимирской области соревнования по компьютерной безопасности CTF проводятся в двух форматах: task-based (или jeopardy) и classic (или классическая игра–attack-defense).

Задумка CTF носит обучающий и соревновательный характер одновременно, что позволяет участникам не только получить опыт в защите и атаке компьютерных систем, но и мотивирует их на достижение лучших результатов. Для решения этих задач участникам приходится применять весь свой запас знаний и совершенствовать его в сферах, связанных с reverse-engineering, исследованием сети, протоколов, администрированием компьютерных систем, приложений и ОС, программированием и т.д.

Формат task-based–игрокам предоставляется набор тасков (заданий), к которым требуется найти ответ и отправить его. Ответ представляет собой «флаг»: это может быть набор символов или произвольная фраза. За верно выполненное задание команда получает определенное количество очков. Чем задание сложнее, тем больше количество очков получит участник в случае правильного ответа (100, 200, 300, 400, 500 очков). Все задания в CTF-соревнованиях формата task-based можно разделить на несколько категорий:

1) admin (задачи на администрирование) – поддержание целостности и работоспособности сети;

2) crypto (криптография) – методы шифрования информации;

3) stegano (стеганография) – скрытие передачи информации путём сохранения в тайне самого факта передачи;

4) web – поиск и анализ веб-уязвимостей;

5) joy – развлекательные задачи разнообразной тематики[2, с. 20];

6) forensic – компьютерно-криминалистическая экспертиза.

Формат classic – каждая команда получает выделенный сервер или небольшую сеть для поддержания её функционирования и защиты от атак соперника. Во время игры команды получают очки за корректную работу сервисов своего сервера и за украденную информацию (флаги) с серверов соперников.

Поставленные задачи являются спецификой специалиста по информационной безопасности.

В настоящее время весьма актуальна концепция защиты информации, в том числе поддержание личной информации в безопасности. Подобные соревнования повышают уровень знаний участников, тем самым вносят изменения их взглядов и предостерегают от случайных действий противоречащего характера в сети Интернет.

За последние годы выявляется тенденция роста популярности движения – CTF в регионе. Задания с каждым разом становятся всё сложнее и интереснее, тем самым привлекая большее количество участников. Первое соревнование CTF состоялось во Владимире в июне 2017 года. Прошло четыре месяца и число желающих выросло в три раза – в этот раз в соревнованиях участвовали 35 команд.

Proceedings of the
Sixth Workshop on Education in Computer Security (WECS) (pp. 17-21). Monterey, CA.

Proceedings of the

Sixth Workshop on Education in Computer Security (WECS) (pp. 17-21). Monterey, CA.

Литература

1. Cheung, R., Cohen, J., Lo, H., Elia, F., & Carrillo Marquez Veronica (2012). Effectiveness of Cybersecurity Competitions. Proceedings of International Conference on Security and Management. LasVegas, Nevada.

2. Eagle, C., & Clark, J. L. (2004). Capture-the-Flag: Learning Computer Security Under Fire. Proceedings of the Sixth Workshop on Education in Computer Security (WECS) (pp. 17-21). Monterey, CA.

3. Irvine C. The value of capture-the-flag exercises in education: An interview with Chris Eeagle. IEEE Security & Privacy, (2011)(pp. 58-60).

Теславская О.И., Солдатова Г.У.,
г. Москва

ОПТИМАЛЬНЫЕ РОДИТЕЛЬСКИЕ СТРАТЕГИИ РЕГУЛЯЦИИ ИСПОЛЬЗОВАНИЯ ДЕТЬМИ ВИДЕОИГР[1]

Увлечение видеоиграми — одно из наиболее популярных в современном мире. В платные сетевые многопользовательские игры наряду со взрослыми играют каждая десятая американская девочка (11%) и почти каждый пятый мальчик (18%) [2]. Обратной стороной всеобщей увлеченности стала обеспокоенность общественности последствиями чрезмерного видеогейминга. В ряде стран (Англии, Южной Корее, Китае, Вьетнаме) на государственном уровне разрабатываются и функционируют программы, осуществляющие лечение и профилактику игровой зависимости. В частности, Конституционный суд Южной Кореи еще в 2014 г. запретил подросткам до 16 лет ночной доступ (с 0:00 до 6:00 утра) к видеоигровым хостингам и установил меру пресечения в виде двух лет лишения свободы либо штраф в размере 10 тыс. долл. США для провайдеров, нарушающих данное постановление [3]. Неудивительно, что сегодня родителей во всем мире интересует вопрос: нужно ли запрещать ребенку играть. Ответ однозначный: не нужно. Даже авторы наиболее радикальных мнений ставят вопрос не о запрете, а о минимизации времени, которое ребенок проводит за видеоигрой. Вопрос не в том, играть или не играть, а в том, сколько детям различных возрастов играть полезно и допустимо или, наоборот, вредно?

Американской педиатрической ассоциацией рекомендуется ограничить время игры 2 часами в сутки – такой умеренный гейминг точно не навредит ребенку, не имеющему серьезных проблем в развитии. При соблюдении нижеуказанных правил он может быть полезен в качестве одного из возможных способов проведения досуга. Оговоримся, что в данном случае речь идет скорее о подростках. Что касается младших школьников, то время игры должно быть ограничено 1часом, причем желательно играть под

[1] Выполнено при поддержке РФФИ (Отделение гуманитарных и общественных наук), заявка №17-06-00762

присмотром или совместно с родителями. Это подтверждается последним Оксфордским исследованием 217 младших школьников 7-8 лет: изучалось количество, качество и тип предпочитаемых игр в качестве предикторов академической успеваемости, вовлеченности в учебный процесс и психического здоровья детей (по оценкам учителей). Выяснилось, что по сравнению с детьми, которые совсем не играют, школьники, играющие немного (около 1часа в день) показали меньший уровень гиперактивности. Дети, которые проводят за играми более 3 часов ежедневно, демонстрируют более высокий уровень гиперактивности и проблемы с успеваемостью по сравнению с неиграющими детьми [8].

Помимо количественных рекомендаций по длительности видеоигры, следует также помнить о других факторах, которые следует учитывать, принимая решение о выборе стратегии родительской медиации в отношении гейминга:

1. Возраст ребенка. Малыши более впечатлительны, их психика только формируется, соответственно, они сильнее подвержены влиянию любых стрессоров, включая видеоигры (в первую очередь со сценами жестокости и агрессии). Соответственно, родителям необходимо как можно тщательнее выбирать игры и жестче контролировать время игрового сеанса. В то же время важно учитывать, что старшие подростки играют значительно дольше и чаще, однако они же более заняты другими видами деятельности (домашние задания, секции, кружки, работа по хозяйству, прогулки и др). Поэтому следует помочь ребенку построить свой распорядок дня таким образом, чтобы время на игру не конкурировало с основными видами деятельности, а было бы моментом отдыха и, возможно, наградой за выполненные обязанности. В целом, если ребенок не испытывает серьезных жизненных трудностей (здоровый сон, хорошая успеваемость, посещение школьных занятий, наличие друзей и интересов), ему можно предоставить большую степень автономии в виртуальном пространстве.

2. Пол ребенка. Исследования убедительно говорят о том, что все эффекты видеоигр куда сильнее сказываются на мальчиках, чем на девочках, поэтому регулирование их деятельности в игровом виртуальном мире должно стать

отдельным фокусом внимания родителей. Мальчики играют значительно чаще и дольше девочек – например, в США консольными увлекается более трети мальчиков, хотя среди девочек таких менее 16% [7]. Мальчики получают больше удовольствия от видеоигр и активно используют их в качестве инструмента социализации, общаясь там со сверстниками [6]. В этом деле серьезной опорой может стать играющий отец (либо другой взрослый, который находится «в теме» видеоигр), который, играя совместно с мальчиком, будет иметь возможность одновременно мягко регулировать степень его увлеченности играми.

3. Место видеоигры в структуре видов активности. Видеоигра должна быть отдельным видом активности, не стоит разрешать ребенку играть параллельно с просмотром мультфильмов, прослушиванием музыки или подготовкой домашнего задания. Изучение индивидуальных различий между подростками 12–16 лет показало, что многозадачность при использовании цифровых технологий в повседневной жизни связана с худшей успеваемостью по математике и английскому языку в классе, худшими показателями рабочей памяти, большей импульсивностью и замедленными темпами развития мыслительных функций по сравнению с остальными детьми [1].

4. Режим дня. Категорически не стоит разрешать детям, в первую очередь, малышам, играть ночью. В 2013 году в экспериментальном исследовании, проведенном на 17 подростках в лаборатории с использованием полисомнографии и метода ведения дневников, было доказано, что, по сравнению с обычной продолжительностью видеоигр перед сном (50 минут), пролонгированное время игры существенно (в среднем на полчаса) снижает длительность и качество сна. Сделан вывод о том, что видеоигры изменяют структуру сна и могут вызывать его нарушения у подростков, причем даже в том случае, если он лег спать вовремя [5]. За час до сна нельзя позволять ребенку использовать любые гаджеты.

5. Одиночный / коллективный характер игропрактики. Стоит включать видеоигры в общую семейную практику развлечений, самим играть с ребенком или, как минимум, интересоваться происходящим в его онлайн-игре. Если ребенок играет в онлайне исключительно с незнакомыми людьми, это повышает склонность к одиночеству и изоляции, а если со знакомыми сверстниками или с

семьей – результатом может стать позитивный сдвиг в общем мироощущении и благополучии ребенка.

6. Жанр игры и специфика игрового контента. Для внимательных родителей сама игра может выступить своего рода диагностикой возможных проблем у подростка. В австрийском исследовании 2011 г. 205 подростков 10–14 лет показало, что конкретные виды видеоигровой продукции идут рука об руку с конкретными проблемами. «Стрелялки» от первого лица чаще выбирают дети, склонные к агрессивному и/или делинквентному поведению, а игры жанра «фэнтези» – дети с интернальными проблемами (стремление к избеганию, уходу от проблем, наличием депрессии / тревожности, соматических симптомов и жалоб)[4].

Литература

1. Cain, M.S., Leonard, J.A., Gabrieli, J.D.E. et al. Media Multitasking in Adolescence // Psychonomic Bulletin & Review, 2016. 23. – pp. 1932-1941.

2. Essential facts about the computer and videogame industry [Электронный ресурс] //USA, Entertainment Software Association, 2017. Available at: http://www.theesa.com/about-esa/essential-facts-computer-video-game-industry (дата обращения: 28.02.2018).

3. Game Shutdown. Constitutional Court in Favor of Banning Nighttime Access to Online Games [Электронный ресурс] // Korea, Premier Business Portal. 2014. URL: http://businesskorea.co.kr/english/news/politics/4303-game-shutdown-constitutional-court-favor-banning-nighttime-access-online-games (дата обращения: 28.02.2018).

4. Holtz P., Appel M.Internet use and video gaming predict problem behavior in early adolescence // Journal of Adolescence. 2011. 34 (1). –pp. 49-58.

5. King, D. L., Gradisar, M., Drummond, A., Lovato, N., Wessel, J., Micic, G., Douglas, P. and Delfabbro, P. The impact of prolonged violent video-gaming on adolescent sleep: an experimental study // Journal of Sleep Research, 2013. 22. – pp. 137–143.

6. Lenhart A., Smith A., Anderson M., Duggan M., Perrin A. Teens, technology and friendships. Video games, social media and mobile phones play an integral role in how teens meet and interact with friends. [Электронный ресурс] // USA, PewResearchCenter, 2015. URL: http://www.pewinternet.org/files/2015/08/Teens-and-Friendships-FINAL2.pdf (дата обращения: 28.02.2018).

7. Media use by tweens and teens [Электронный ресурс] // USA, Common Sense Media. 2015. URL: https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens (дата обращения: 28.02.2018).

8. Przybylski A., Mishkin A. How the quantity and quality of electronic games relates to adolescents' academic engagementand psychological adjustment // Psychology of popular media culture. 2016. Vol. 5. No 2. – pp. 145—146.

Волчек В.Н.,
г. Москва

ПРОБЛЕМА ОТЦОВ И ДЕТЕЙ В ЭПОХУ ИНТЕРНЕТА

Проблема поколений не нова. Но есть у текущего времени своя особенность — это Интернет. Большинство детей проводит уйму времени в социальных сетях. Не меньше времени за компьютером/планшетом/телефоном проводят и их родители. Вся разница лишь в том, что взрослые и дети обитают на разных площадках.

Дети подвержены влиянию субкультур и копируют поведение своих кумиров. Еще 20 лет назад, вопрос контроля за увлечением детей, особенно подростков, был затруднен. Детей воспитывала улица или телевизор. Ни те, ни другие практически не подчинялись родительскому контролю, но самое главное, влияние субкультур происходило скрыто от взрослых. Достать информацию и разобраться в том или ином молодежном движении было практически невозможно. Сегодня ситуация кардинально поменялась.

Изучение субкультуры ребенка — залог его безопасного развития.

Поясним на примере увлечения крайне популярным среди подростков хип-хопом. Почему крайне важно разбираться в увлечениях ребенка? Любая субкультура имеет две стороны медали. Увлечение хип-хопом для одних заканчивается наркотиками, для других выступлением на Олимпийский играх (брейк-данс теперь олимпийский вид спорта) или продаже картин с граффити в каталогах ведущих галерей современного искусства. Поэтому крайне важно разбираться в субкультуре, завладевшей умом ребенка, чтобы понимать всевозможные риски и последствия, а также вовремя поспособствовать развитию увлечения в положительном продуктивном русле.

Благодаря Интернету теперь стало намного проще получать информацию о том или ином увлечении ребенка. Можно изучать лидеров мнений, знакомиться со знаковыми событиями и мероприятиями, важными для ребенка. Изучая увлечение ребенка, взрослый становится ближе. Так, например, необычайно быстро набравший популярность на YouTube канал «Вдудь», добился успеха за

счет того, что стал показывать взрослой аудитории подростковых Интернет-кумиров. Как отмечают, сами зрители данного интернет-канала: «Наконец-то стало, о чем поговорить с детьми».

В один промежуток времени, мы, очевидно, потеряли контакт с детьми. Интернет — будучи свободно наполняемой и неконтролируемой сетью привел к ситуации, когда взрослые потеряли своих детей во Всемирной паутине, при этом сами многие из взрослых запутались в ней не меньше детей, но просто на другом конце. Сегодняшним родителям нужно встретиться с детьми в онлайне. Только имея глубокое понимание, чем живут дети в сети, можно уберечь ребенка от пагубного влияния, памятуя при этом, что далеко не все кажущиеся на первый взгляд негативные и непонятные вещи в субкультурах, являются таковыми. И различать это возможно только тогда, когда вы сами погрузились в субкультуру ребенка.

С детьми разговаривать надо на их языке, а в сегодняшнем лексиконе там преобладают слова, типа «Эшкере», «Хайп», «Лойс» и «Зашквар», пришедшие к нам из среды видеоблоггинга. Понимание значения этих слов в купе с их уместным употреблением раскрепощает детей и располагает их к общению.

Правила безопасной работы в Интернете.

Детей, равно как и взрослых, необходимо обучать безопасной работе в сети Интернет. Рассмотрим некоторые из методик позволяющие обезопасить себя и детей при работе в Интернете.

- Не делайте из личных данных публичные.

Опросы в школах показывают, что дети зачастую имеют открытые профили в социальных сетях, где они собственноручно разместили свой домашний адрес, адрес школы, свои взгляды, работу родителей и т. д. Делая свои данные публичными, дети, равно как и взрослые, становятся легкой добычей для мошенников. Нужно с детства прививать понимание целесообразности раскрытия своих персональных данных на просторах Интернета. В связи с этим рекомендуется научить ребенка отвечать на следующие вопросы при размещении информации во Всемирной Паутине:

– Зачем Вам открытая для всех социальная страница?

- Зачем Вы указали свое местожительство, место работы и место учебы?
- Зачем Вы рассказываете о своих перемещениях?
- Зачем Вам геометки в постах и фотографиях?

Истории «Синего Кита», похищения Ивана Касперского — сына создателя знаменитой антивирусной программы, рекомендации Росгвардии не публиковать новости о предстоящем отпуске за границей — все это подчеркивает важность правила «Не делайте из личных данных публичные».

- Все, что Вы напишите в Интернете, останется там навсегда.

Сервисы, подобные web.archive.org сохраняют состояние страниц на долгие годы. Кроме того, состояние страниц кэшируют поисковики, различные аналитические компании, да и сами социальные сети не торопятся удалять Вашу информацию, даже если Вы нажали кнопку «Удалить» и уже потеряли доступ к недавно загруженной фотографии — в большинстве случаев физически с сервера она не удаляется. Вся эта информация сегодня представляет огромный интерес для маркетологов. Поэтому нужно объяснить детям простую мысль - все, что вы напишите или выложите в Интернете, останется там навсегда.

Долгое время Интернет был не подконтрольной средой общения, в которой допускались совершенно любые высказывания. Чувство безнаказанности пронизало всю сеть, однако, на сегодняшний момент, ситуация изменилась в корне. Все, сказанное в сети, может иметь самые разные последствия - от отдаленных личных проблем, до уголовной ответственности уже сегодня.

На сегодняшний день в России запрещены публикации, способствующие распространению наркотиков и детской порнографии, склонение к суициду, а также призывы к массовым беспорядкам. Все это законодательно запрещено писать в социальных сетях и блогах. Но нужно также иметь в виду, что любая травля или оскорбление человека в Интернете тоже может закончиться уголовным преследованием. Учитывая появление так называемого «кибербуллинга», представляется необходимым разъяснять последствия данного явления детям. Зачастую, родители и учителя не знают, как помочь жертве кибербуллинга – однако решение на поверхности - нужно немедленно обращаться

в полицию. Границы между онлайн жизнью и офлайн на самом деле давно отсутствуют.

Другой стороной проблемы является развитие сервисов скрининга на планете. Данные сервисы позволяют на основании информации в Сети, в том числе публичных постов и комментариев, в автоматическом режиме собрать портрет человека. Работодатели, банки, арендодатели уже во всю пользуются данными сервисами, и, если там найдется компромат — это все может иметь негативные последствия для человека. Поэтому крайне важно сдерживать себя и свои эмоции в сети, особенно при общении с так называемыми «троллями», задача которых вывести человека из себя - «потроллить». Популярная в Интернете фраза «Не кормите троллей» - сегодня актуальная как никогда.

Еще одной проблемой является проблема перепостов. Вы можете даже ничего не писать, но разместив информацию, опубликованную кем-то другим у себя на странице, Вы точно также несете полную ответственность. В этом плане крайне важно привить детям навыки распознавания «фейков», который заключается в поиске и проверке первоисточника. Если первоисточник найти не удается, или он не заслуживает доверия, лучше избежать так называемого «перепоста», даже если он вызвал в Вас сильные эмоции. Кстати, сильная эмоция, возникшая после просмотра видеоролика или прочтения статьи, также является типичным маркером «фейка» - за счет этого они имеют скоростное массовое распространение.

Также необходимо отметить важность приватности в сети. Методы социальной инженерии позволяют современным хакерам взламывать странички социальных сетей, не применяя технических средств. Здесь действует одно правило — всегда помните, что даже самый близкий друг, общаясь с Вами в сети, может оказаться не им самим. Страницы взламываются, специалисты по социальной инженерии мимикрируют под реальных людей. Поэтому если Вы чувствуете, что собеседник ведет себя нетипично, лучше верифицировать его, например, позвонив на сотовый телефон и убедиться, что это именно он общается в данный момент с Вами.

Кроме того, необходимо изучение способов технической защиты от взлома, такие как:

- Использование надежных и разных паролей на разных сервисах
- Контроль URL, во избежание перехода по так называемым фишинговым сайтам
- Предпочтение протоколу HTTPS, вместо HTTP
- Контроль установки сторонних приложений или расширений браузера.

Перечисленные выше методы являются базовыми, однако, их число гораздо больше и обзор данных средств защиты выходит за рамки данной статьи.

Интернет-фильтры

Интернет-фильтры не дают гарантии безопасной работы в сети для ребенка. Более того, существует огромное количество возможностей обойти любое ограничение в сети. Все зависит от технической квалификации. Так как в большинстве случаев, дети сегодня намного более подкованные, чем взрослые при работе за компьютером, излишне полагаться на блокировщики контента не следует.

Платные Интернет - фильтры хорошо справляются с защитой от нежелательного контента, такого как порнография, однако стоят они весьма дорого, и имеют множество ложных срабатываний. Тем не менее их применение оправданно, если ребенок уже подсел на «иглу» Интернета. Существуют также более мягкие бесплатные интернет-фильтры, такие как Яндекс.DNS. Данный сервис не гарантирует 100% защиты от порнографии, однако является абсолютно бесплатным и имеет минимум ложных срабатываний. Настроив, Яндекс.DNS на интернет-маршрутизаторе в квартире ребенка, домашняя сеть будет надежно защищена от большинства негативных факторов. Однако следует осознавать, что домашний Интернет сегодня не является единственным каналом связи для ребенка. Другим каналом является сотовая связь. Поэтому выбирая сотового оператора, нужно отдавать предпочтение специальным детским тарифам, и ни в коем случае не покупать ребенку безлимитный мобильный Интернет без необходимости.

Но есть в России одна нерешаемая проблема — социальная сеть «ВКонтакте». Эта самая популярная социальная сеть России содержит огромное количество порнографического контента, и, судя по всему, разработчики не желают принимать достаточные усилия для решения этой проблемы. Интернет-фильтры, такие как Яндекс.DNS, не блокируют «ВКонтакте» и дети получают неограниченный доступ к видео порнографического характера. Все это нужно учитывать, создавая себе и своим детям страницы в данной социальной сети. Другие социальные сети, менее подвержены распространению порнографии и нелегального контента, чем «ВКонтакте». «ВКонтакте» - единственная из крупнейших социальных сетей мира, которая хранит петабайты нелегального порно и прочего нелегального контента.

Только изучив среду, в которой обитает Ваш ребенок, осознав риски и возможные последствия, можно принимать меры по обеспечению безопасности в сети. Перечисленные в статье меры способны существенно снизить риск потенциальных проблем, связанных с времяпрепровождением в сети. Главное нужно осознавать, что Интернет — это всего лишь инструмент, и во многом от взрослых зависит , сможем ли мы использовать его во благо наших детей.

Монахов М.Ю.,
г. Владимир

ИНФОРМАЦИОННОЕ ПРОТИВОДЕЙСТВИЕ НЕГАТИВНЫМ ТЕНДЕНЦИЯМ В ПРОЦЕССЕ ФОРМИРОВАНИЯ ГЛОБАЛЬНОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА

Благодаря развитию ИТ формируется глобальное информационное общество, в котором присутствуют информационные ценности разных народов, принципиально изменяется форма и оперативность процесса общения людей. Осознавая новые возможности и перспективы, открываемые данным процессом, следует понимать, что существуют и негативные тенденции, и аспекты процесса глобализации.

Это все существенно повышает зависимость безопасности общества, каждого конкретного человека от качества функционирования информационной инфраструктуры, достоверности, целостности используемой информации, ее защищенности от несанкционированной модификации, а также противоправного доступа к ней.

Чтобы получить метод противодействия данным негативным тенденциям, необходимо определиться с объектом защиты, злоумышленниками, их угрозами, методами и средствами атак, возможными механизмами защиты.

Пусть в данной связи, объектами защиты будут индивидуальное, групповое и массовое сознание людей, которое подвергается агрессивным информационным воздействиям.

Защита выделенных объектов от противоправных информационных воздействий – угроз - составляет основное содержание деятельности по обеспечению информационно-психологической безопасности - нового и еще недостаточно разработанного направления обеспечения ИБ.

Объект «Индивидуальное сознание».Под данным объектом информационно-психологической безопасности будем понимать способность человека адекватно воспринимать окружающую действительность, свое место во внешнем мире,

формировать в соответствии со своим жизненным опытом определенные убеждения и принимать решения в соответствии с ними.

Основными угрозами являются целенаправленно осуществляемые людьми или техническими средствами информационные воздействия, направленные на сознание и подсознание человека, и проводимые без его согласия. Угрозы имеет целью изменить психические реакции и поведение человека.

Злоумышленники. Существенную опасность представляют интенсивно действующие в России религиозные секты и группы, проповедующие фанатизм, экстремизм и человеконенавистничество. Одним из источников угроз индивидуальному сознанию российских граждан, многие из которых находятся за чертой бедности и не имеют устойчивых средств к существованию, является агрессивная реклама дорогостоящих товаров, навязывающая установки на вхождение в «элиту» любыми способами. Не менее опасными являются представители «оккультных наук», в изобилии предлагающие гражданам свои услуги «по снятию сглаза и порчи». Следствием проявления данной угрозы может быть, как нарушение психического здоровья людей, так и действия граждан во вред интересам общества и государства.

Объект «Групповое сознание». Под данными будем понимать общие интересы группы, составляющие цель ее создания, принятые и осознанные членами группы правила поведения.

В соответствии с Конституцией граждане имеют право свободно объединяться. Исключение составляют общественные объединения, цели и действия которых направлены на насильственное изменение основ конституционного строя, на создание вооруженных формирований, разжигание расовой, национальной розни.

Угрозы групповому сознанию могут проявляться в виде противоправных информационных воздействий со стороны других групп, общественных или государственных организаций с целью разрушения общности интересов группы, созданию трудностей на пути реализации этих интересов, дискредитации членов группы, оказания психологического давления на них.

Источниками угроз являются другие группы (религиозные, этнические). Способы воздействия - недобросовестная конкуренция, конфронтационные отношения.

Следствием проявления угроз может явиться распад группы, нарушение взаимодействия с другими группами, общественными и государственными организациями, т.е. по существу, препятствие реализации упомянутой статьи Конституции РФ.

Объект «Массовое сознание». Под данным объектом будем понимать: общие интересы больших масс граждан (социальных групп, национальных образований, наций, населения страны в целом); признаваемые ими культурные, духовные и нравственные ценности, правила поведения и образ жизни; готовность к противодействию существующим угрозам этим интересам, ценностям и нравам.

Угрозы заключаются, прежде всего, в искажении информации о происходящих событиях, манипулировании данной информацией с целью формирования необходимой эмоциональной оценки заданных событий.

Следствием проявления этих угроз является нарушение массового сознания данной человеческой ассоциации восприятия окружающей действительности. Неадекватность восприятия в зависимости от установившихся стереотипов поведения в данной ассоциации может проявляться в форме социальной апатии или агрессивности по отношению к внешнему миру.

Злоумышленники – противники нашего государства, политические противники и т.д. Замечу, что в условиях продолжающегося экономического кризиса и неразвитости гражданского общества в России конкретные угрозы они черпают в неопределенности нравственных ценностей, защищаемых государством, в несогласованности действий органов государственной власти и общественных организаций.

Обеспечение информационно-психологической безопасности предполагает формирование соответствующей системы противодействия выделенным угрозам.

Нормативно-правовая составляющая обеспечивает формирование и совершенствование системы правовых норм противодействия угрозам информационно-психологической безопасности и механизмам их реализации.

Она образуется совокупностью нормативных правовых актов, других нормативных документов, регулирующих отношения в области выявления угроз и противодействия этим угрозам, обеспечивающего реализацию конституционных прав и свобод, их законных ограничений, охрану психического здоровья граждан, сохранение социального спокойствия в обществе.

Организационная составляющая устанавливает функциональную структуру общественных организаций и государственных органов, занимающихся реализацией правовых норм в данной области, и отношения между ними, а также между этими организациями и органами, с одной стороны, и гражданином - с другой. Представляется, что важнейшей частью организационной составляющей системы должны быть соответствующие структуры гражданского общества.

Технологическая составляющая обеспечивает возможность свободного и безопасного информационного обмена между гражданами, членами групп и групповых ассоциаций и предотвращения противоправного информационного воздействия на них. Она должна обеспечить возможность своевременного выявления возникающих угроз информационно-психологической безопасности личности, общества и государства, оценку возможного и нанесенного ущерба этой безопасности и организации эффективного противодействия данным угрозам.

Кадровая составляющая призвана обеспечить формирование и поддержание достаточного кадрового потенциала общества и государства для эффективного функционирования системы обеспечения информационно-психологической безопасности.

Тельный А.В.,
г. Владимир

ДЕЯТЕЛЬНОСТЬ СПЕЦИАЛИСТА ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Целью данной статьи является обзор трудовых функций и примерных должностных обязанностей специалиста по технической защите информации согласно требованиям действующего профессионального стандарта, а также краткая формулировка направлений научных исследований в профессиональной деятельности специалиста по технической защите информации.

Сферы деятельности специалистов по технической защите информации определены профессиональным стандартом 06.034 «Специалист по технической защите информации», зарегистрировано в Минюсте России 25 ноября 2016 г. N44443 [1]. Основная цель вида профессиональной деятельности - предотвращение утечки информации ограниченного доступа по техническим каналам в результате несанкционированного доступа к информации и специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней.

Стандарт 06.034 «Специалист по технической защите информации»

Укрупненная трудовая функция	Образование	Наименование занимаемой должности
Проведение работ по установке и техническому обслуживанию средств защиты информации	Среднее профессиональное образование - программы подготовки специалистов среднего звена	Техник по технической защите информации I – II категории; Техник по технической защите информации
Проведение работ по установке и техническому обслуживанию защищенных технических средств обработки информации	Высшее образование - бакалавриат в области информационной безопасности	Специалист по технической защите информации I –II категории; Специалист по технической защите информации Инженер по технической защите информации
Производство, сервисное обслуживание и ремонт средств защиты информации	Высшее образование - бакалавриат в области информационной безопасности	Специалист по технической защите информации I –II категории; Специалист по технической защите информации Инженер по технической

		защите информации
Проведение контроля защищенности информации	Высшее образование - бакалавриат в области информационной безопасности	Специалист по технической защите информации I –II категории; Специалист по технической защите информации Инженер по технической защите информации
Разработка средств защиты информации	Высшее образование - специалитет или магистратура в области информационной безопасности	Специалист по технической защите информации I –II категории; Специалист по технической защите информации Инженер по технической защите информации
Проектирование объектов в защищенном исполнении	Высшее образование - специалитет или магистратура в области информационной безопасности	Специалист по технической защите информации I –II категории; Специалист по технической защите информации Инженер по технической защите информации
Проведение аттестации объектов на соответствие требованиям по защите информации	Высшее образование - специалитет или магистратура в области информационной безопасности и дополнительное профессиональное образование - программы повышения квалификации (ППК)	Специалист по технической защите информации I –II категории; Специалист по технической защите информации Инженер по технической защите информации
Проведение сертификационных испытаний средств защиты информации на соответствие требованиям по безопасности информации	Высшее образование - специалитет или магистратура в области информационной безопасности и ППК	Специалист по технической защите информации I –II категории; Специалист по технической защите информации Инженер по технической защите информации
Организация и проведение работ по технической защите информации	Высшее образование - специалитет или магистратура в области информационной безопасности и дополнительное профессиональное образование ППК или Высшее образование - аспирантура (адъюнктура)	Главный специалист по технической защите информации Руководитель структурного подразделения по технической защите информации

Основные должностные обязанности специалиста по технической защите информации

– Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.

– Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты акустической речевой информации от утечки по техническим каналам.

– Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программно-технических средств защиты информации от несанкционированного доступа.

– Проведение работ по установке, настройке и испытаниям защищенных технических средств обработки информации.

– Проведение работ по техническому обслуживанию защищенных технических средств обработки информации.

– Производство, сервисное обслуживание и ремонт технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.

– Производство, сервисное обслуживание и ремонт технических средств защиты акустической речевой информации от утечки по техническим каналам.

– Производство, сервисное обслуживание и ремонт программно-технических средств защиты информации от несанкционированного доступа.

– Производство, сервисное обслуживание и ремонт защищенных технических средств обработки информации.

– Производство, сервисное обслуживание и ремонт технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок.

– Производство, сервисное обслуживание и ремонт технических средств контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам.

– Производство, сервисное обслуживание и ремонт программно-технических средств контроля защищенности информации от несанкционированного доступа.

– Проведение специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации.

– Проведение контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок.

– Проведение контроля защищенности акустической речевой информации от утечки по техническим каналам.

– Проведение контроля защищенности информации от несанкционированного доступа.

– Разработка технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.

– Разработка технических средств защиты акустической речевой информации от утечки по техническим каналам.

– Разработка программно-технических средств защиты информации от несанкционированного доступа.

– Разработка технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок.

– Разработка технических средств контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам.

– Разработка программных (программно-технических) средств контроля защищенности информации от несанкционированного доступа.

– Проектирование средств и систем информатизации в защищенном исполнении.

– Проектирование систем защиты информации на объектах информатизации.

– Проектирование выделенных (защищаемых) помещений.

– Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации.

– Проведение аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации.

– Проведение сертификационных испытаний на соответствие требованиям безопасности информации технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.

– Проведение сертификационных испытаний на соответствие требованиям безопасности информации технических средств защиты акустической речевой информации от утечки по техническим каналам.

– Проведение сертификационных испытаний на соответствие требованиям по безопасности информации программных (программно-технических) средств защиты информации от несанкционированного доступа.

– Проведение сертификационных испытаний на соответствие требованиям по безопасности информации технических средств обработки информации в защищенном исполнении.

– Проведение сертификационных испытаний на соответствие требованиям по безопасности информации технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок.

– Проведение сертификационных испытаний на соответствие требованиям по безопасности информации технических средств контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам.

– Проведение сертификационных испытаний на соответствие требованиям по безопасности информации программных (программно-технических) средств контроля защищенности информации от несанкционированного доступа.

– Создание системы защиты информации в организации.

– Ввод в эксплуатацию системы защиты информации в организации.

– Сопровождение системы защиты информации в ходе ее эксплуатации.

Направления научных исследований по направлению деятельности специалиста по технической защите информации

– Математическое моделирование функционирования технических средств инженерно-технической защиты объектов.

– Математическое моделирование функционирования технических средств защиты объектов от утечки информации по техническим каналам.

– Исследование достаточности технических средств инженерно-технического укрепления объектов.

– Моделирование функционирования технических средств охранно-тревожной сигнализации.

– Моделирование функционирования систем контроля и управления доступом.

– Моделирование функционирования систем охранного телевидения.

– Моделирование обеспечения защиты от несанкционированного доступа (НСД) при комплексном оборудовании объекта средствами инженерно-технической защиты.

– Моделирование утечки информации по линиям телекоммуникаций, выходящих за пределы контролируемой зоны.

– Математическое моделирование каналов утечки информации.

– Разработка методик определения контролируемой зоны объекта.

– Методы и алгоритмы повышения качества взаимодействия подсистем безопасности для интегрированных систем безопасности.

– Разработка новых методов, алгоритмов и технических средств обнаружения несанкционированного доступа на объект.

– Разработка моделей и алгоритмов обеспечения безопасности каналов передачи данных в информационно-телекоммуникационной сети комплексной системы охраны и безопасности предприятия.

– Разработка моделей и алгоритмов контроля каналов передачи данных системы передачи извещений при централизованной охране объектов.

– Автоматизация проектирования инженерно-технических средств.

– Разработка новых методов, алгоритмов и технических средств повышения надежности функционирования средств инженерно-технической защиты объектов.

– Разработка новых методов, алгоритмов и технических средств обнаружения террористически опасных объектов и предметов.

– Разработка новых методов, моделей и алгоритмов оптимизации размещения технических средств телекоммуникаций и защиты информации на основе анализа архитектурно - планировочных решений проектируемых объектов.

– Защита телекоммуникационных сетей и кабельных коммуникаций от утечки информации по техническим каналам.

– Исследование защищенности каналов связи систем передачи извещений при осуществлении централизованной охраны объектов.

– Разработка новых организационных средств и методов совершенствования функционирования службы охраны и безопасности объекта.

– Разработка методик прогнозирования успешности действий нарядов физической охраны по предотвращению несанкционированного доступа нарушителя на охраняемый объект.

– Разработка методик аудита состояния инженерно-технической защиты объекта.

– Разработка математических критериев оптимальности оснащения объекта средствами инженерно-технической защиты.

– Разработка методов и технических решений построения оптимальной структуры интегрированных систем безопасности объектов.

– Разработка методик технико-экономического обоснования выбора проектных решений оснащения объектов инженерно-техническими средствами защиты.

– Разработка технических средств защиты платежных систем.

Литература:

1. Профессиональный стандарт 06.034. Специалист по технической защите информации : зарегистрировано в Минюсте России 25 ноября 2016 г. № 44443.

2. Тельный, А. В. Оценка защищенности информационных ресурсов организации от несанкционированного доступа нарушителей в здания и помещения / А. В. Тельный, Ю. М. Монахов, М. Ю. Монахов // Известия высших учебных заведений. Технология текстильной промышленности. – 2016. – № 5. – С. 259-263.

3. Тельный А. В. Автоматизация оценки достаточности технических средств охраны и безопасности для защиты от несанкционированного доступа производственного объекта / А. В. Тельный, Ю. М. Монахов, М. Ю. Монахов // Известия высших учебных заведений. Технология текстильной промышленности. – 2016. – № 5. – С. 263-267.

4. Тельный А. В. Формирование динамической модели оценки показателей надежности объектовых комплексов технических средств охранной сигнализации / А. В. Тельный, М. Ю. Монахов // Динамика сложных систем – XXI век. – 2015. – № 4. – С. 34-41.

Мишин Д.В., Абрамова О.И., Сорокина М.А., Марцева А.Е.,

г. Владимир

ОБ ОСОБЕННОСТЯХ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СРЕДЫ СРЕДНИХ ОБЩЕОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ ВЛАДИМИРСКОЙ ОБЛАСТИ

Все муниципальные средние общеобразовательные школы (далее – образовательные организации - ОО) Владимирской области, использующие информационные системы (ИСОО) для обработки конфиденциальной информации, обязаны обеспечивать защиту этой информации в соответствии с Законом. Авторы выделяют следующие структурные и функциональные особенности типовой ИСОО, которые необходимо учитывать при построении системы защиты информации ИСОО:

1. Информационная среда ОО, как правило, многокомпонентная - состоит из нескольких подсистем, обрабатывающих персональные данные (ПДн)различных категорий и другую конфиденциальную информацию.

2. В некоторых случаях требуется обеспечение целостности и доступности, как защищаемой информации (например, официального сайта ОО), так и элементов ИТ-инфраструктуры ИСОО, средств защиты информации (СЗИ) и средств криптографической защиты информации (СКЗИ), в случаях применения таковых.

3. Различные подсистемы ИСОО могут функционировать на базе единой ИТ-инфраструктуры ОО т.е. отдельные средства вычислительной техники (СВТ) применяются для обработки защищаемой информации различной степени конфиденциальности в рамках различных подсистем ИСОО.

4. Обработкой конфиденциальной информации в ИСОО занимаются сотрудники ОО (руководство, педагогический состав), большинство из которых не имеют достаточных знаний в области защиты информации. Случаи наличия в штате ОО сотрудника, имеющего профильное образование (профессиональная

переподготовка) в области обеспечения ИБ, крайне редки (такие случаи следует рассматривать, скорее, как исключения из общих правил).

По результатам аудита десяти ОО Владимирской области и с учетом вышеописанных особенностей ИСОО, можно утверждать, что:

1. Все ОО Владимирской области являются операторами ПДн, следовательно, обязаны обеспечивать защиту ПДн в соответствии с положениями Федерального закона № 152-ФЗ «О персональных данных» и принятых во исполнение его подзаконных актов:

- Постановление Правительства РФ (ПП) РФ N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- ПП РФ N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- ПП РФ N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказ ФСТЭК № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Специальные требования и рекомендации по технической защите конфиденциальной информации».

2. В связи с подключением АРМ администраторов АИС к защищенной сети системы образования и ГИС РС «Контингент», ОО обязаны реализовать меры обеспечения безопасности данных АРМ в соответствии с требованиями

законодательства РФ по защите информации в ГИС (№ 149-ФЗ «Об информации, информационных технологиях и о защите информации»):

- ПП N 555 «О внесении изменений в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
- ФСТЭК Приказ N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- ФСТЭК «Методический документ. Меры защиты информации в государственных информационных системах».

3. В связи с применением для защиты ПДн средств криптографической защиты информации (применение СКЗИ связано с защитой каналов связи или/и применением электронной подписи (ЭП)), ОО обязаны (в дополнение к прочим мерам) реализовать организационные и технические меры, утвержденные соответствующими актами ФСБ:

- Приказ ФАПСИ N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ ФСБ N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Приказ ФСБ N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации»;

- «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности».

Логинова Н.А.,
г. Суздаль

МЕРЫ СНИЖЕНИЯ УГРОЗ УЧАСТНИКОВ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА В СЕТИ ИНТЕРНЕТ

«…Так вот, жил-был тролль, злющий - презлющий; то был сам дьявол. Раз он был в особенно хорошем расположении духа: он смастерил такое зеркало, в котором всё доброе и прекрасное уменьшалось донельзя, всё же негодное и безобразное, напротив, выступало ещё ярче, казалось ещё хуже…

Все ученики тролля — у него была своя школа — рассказывали о зеркале, как о каком-то чуде.

— Теперь только, — говорили они, — можно увидеть весь мир и людей в их настоящем свете!

И вот они бегали с зеркалом повсюду; скоро не осталось ни одной страны, ни одного человека, которые бы не отразились в нём в искажённом виде…»

(Из сказки Г.Х.Андерсена Снежная королева)

Интернет является неотъемлемой частью жизни не только взрослого человека, но и современных детей. Он предлагает много интересных возможностей и занимает одно из центральных мест в нашей ежедневной реальности. Современный молодой человек чувствует себя неуютно, если не может воспользоваться сервисами сети Интернет. Порой трудно увидеть грань перехода от реальности к виртуальности.

Дети и подростки пользуются Интернетом для общения, игр, обмена, поиска информации, для получения помощи и консультаций при выполнении домашних заданий, при подготовке к экзаменам и для многих других целей. Дети выполняют все информационные процессы, прибегая к ресурсам сети. Информация, как пища, может быть полезной – во благо, а может быть вредной. Поэтому обеспечение информационной безопасности учащихся поднимается и на государственном уровне, и в среде педагогов, и в среде родителей.

Как же защитить ребенка от опасностей в сети? Классификаций интернет-рисков существует несколько. Я придерживаюсь классификации предложенной Фондом Развития сети Интернет:

контентные риски возникают в процессе использования находящихся в Сети материалов (текстов, картинок, аудио- и видео файлов, ссылок на различные ресурсы), содержащих противозаконную, неэтичную и вредоносную информацию;

коммуникационные риски возникают в процессе общения и межличностного взаимодействия пользователей в Сети (кибербуллинг, груминг, домогательства);

потребительские риски возникают в процессе приобретения товаров и услуг через Интернет (приобретения товара низкого качества, контрафактной и фальсифицированной продукции, потери денежных средств без приобретения товара или услуги, хищения финансовой информации с целью мошенничества);

технические риски определяются возможностями повреждения программного обеспечения компьютера, хранящейся на нем информации, нарушения ее конфиденциальности или взлома аккаунтов, хищения паролей и персональной информации посредством вредоносных программ (вирусов, червей, троянских коней, шпионских программ, ботов и др.)

Поэтому одной из важной задач школы, любого учителя, классного руководителя становится обучение методам поиска в сети Интернет информации достоверной, объективной, актуальной, полной. Научить пользоваться ресурсами сети, не нанося себе и окружающим вреда. Детей надо учить правилам безопасного поведения в сети, как правилам поведения и пребывания в общественных местах, на дорогах.

Особенность обучения информационной безопасности связана с использованием технических, организационных средств защиты личности, в совокупности с нравственно-этическим и правовым аспектом использования информации.

Если технические, правовые меры контролирует государство с помощью ФЗ, то организационные средства и нравственно-этическая сторона это инициатива и выбор стратегии учебного заведения.

Что может сделать школа, чтобы снизить угрозы сети для участников образовательного процесса? Развитие критической оценки информации, формирование умения распознавать манипулирование, причиняющего вред психическому и физическому здоровью; обучение мерам самозащиты от нежелательного контента и контактов в сетях в компетенции любой школы.

Можно предложить ряд рекомендаций:

- разработать правила и процедуры использования интернета в образовательном учреждении, регулярно оценивать и пересматривать их эффективность совместно с родительским советом школы. (Инструкция по ТБ и приложение к уставу);

- обеспечить осведомленность о правилах использования ИКТ (недели безопасного Интернета; страницы безопасности школьного сайта; создание школьной сети для совместной работы учителей и учащихся; в рамках внеурочной деятельности можно вести курс «Безопасного поведения учащихся в сети», тем более, что существуют даже теоретические и практические пособия для таких занятий, разработанные, к примеру, фондом развития Интернет; круглые столы, лектории тренинги для родителей, учителей);

- назначить координатора действий по обеспечению информационной безопасности;

- прибегать к услугам лицензированного поставщика услуг интернета;

- использовать программные продукты фильтрации и мониторинга сети;

- обеспечить обучение всех детей навыкам электронной безопасности. (включить в календарно-тематическое планирование Единый урок безопасности в сети; организовывать квесты, игры для формирования навыка безопасной деятельности в сети);

- обеспечить обучение и повышение квалификации коллектива в области электронной безопасности;

организовать в школе пункт приема обращений, для сбора информации о нарушений информационной безопасности. Регистрировать и реагировать на

происшествия. Анализировать и оценивать риски связанные с появляющимися новыми технологиями.

Ближе всего к учащимся находится учитель, классный руководитель. В помощь учителю разработаны многочисленные ресурсы:

– Все о безопасном Интернете на Информационном портале школьных библиотек России http://www.rusla.ru/rsba/technology/safety/

– Сайт фонда развития Интернет. Дети России Онлайн. Здесь вы найдете методические и дидактические материалы; статистические данные, образовательные проекты для учителей, детей, родителей, вас проконсультируют по проблемам безопасного использования интернета и мобильной связи. На Линии помощи профессиональную психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М.В.Ломоносова и Фонда Развития Интернет. http://www.detionline.com/

– Интернет-игра по информационной безопасности http://igra-internet.ru/game.

– Игра для детей 7-10 лет "Через Web джунгли". http://www.wildwebwoods.org/popup.php?lang=ru

– Образовательный проект МТС «Дети в Интернете» разделе «Уроки» предлагает дидактический материал для проведения урока безопасности в сети, методическое пособие, брошюру для родителей, онлайн игру http://detionline.com/mts/aboutв.

– Проект «Разбираем Интернет» рассказывает об устройстве электронного мозга сетевого пространства, дети узнают, как получить доступ к знаниям, находить нужную информацию, критически оценивать контент, создавать собственные Интернет-проекты, общаться, соблюдая правила безопасности http://www.razbiraeminternet.ru/

– Портал Персональные данные содержит материалы, которые были разработаны специалистами Роскомнадзора в помощь участникам образовательного процесса. Портал призван помочь детям понимать последствия, которые информационные технологии могут оказать на личную жизнь. http://персональныеданные.дети/

– Сделайте Интернет безопасным для своих детей. Содержит информацию об основах безопасности в сети, описание и инструменты для обеспечения безопасности детей в Интернете от Google https://www.google.ru/safetycenter/families/start

– Securelist (современные угрозы, аналитика, статистика, глассарий, описания и блог от Лаборатории Касперского) http://www.securelist.com/ru/

– Лаборатория Касперского для образования http://academy.kaspersky.ru/

Учитель, классный руководитель сегодня имеет мощный инструмент в выстраивании межличностных отношений, организации современных и интересных для поколения-Z форм и методов взаимодействий в рамках и за рамками образовательного процесса. Таким как онлайн-обучение, наставничество и исследовательская учебная деятельность в сети, использование альтернативных образовательных источников информации. Учебная среда из ограниченного классно-урочного пространства расширилось до сообществ, участники которых занимаются, общаются и сотрудничают виртуально, оставаясь круглосуточно на связи благодаря социальным сетям.

Умело пользоваться благами ресурсов сети Интернет должны научить учителя. Обучение письменной грамотности и информационной грамотности должно осуществляться одномоментно общими усилиями профессионалов и неравнодушных родителей.

Федорова Е.В.,
г. Владимир

ВЛИЯНИЕ СОВРЕМЕННЫХ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ НА ОБРАЗ ЖИЗНИ, ВОСПИТАНИЕ И ЛИЧНОСТНОЕ СТАНОВЛЕНИЕ ПОДРАСТАЮЩЕГО ПОКОЛЕНИЯ

Современное общество, наверное, сложно представить без компьютеров, телефонов, планшетов. Все эти вещи, а также интернет и телевидение, настолько плотно вошли в нашу жизнь, что порой кажется, что без них не обойтись.

Но давайте с вами задумаемся о том, а какое же все-таки влияние на подрастающее поколение оказывают современные инфокоммуникационные технологии?

Любое влияние может быть как положительным, так и отрицательным. И это зависит не столько от того, что нам показывают, но и от того, как мы к этому относимся, какой выбор мы делаем.

Другими словами, если мы, например, в интернете посмотрим передачу про животных, то никакого негативного влияния она на нас, скорее всего, не произведет. Но если мы, например, решили посмотреть видеоролики со сценами насилия, жестокости или прочитать статью об этом, то можно с уверенностью сказать, что такой просмотр окажет негативное и пагубное влияние на нас.

Но, задайте сами себе вопрос – Кто делает выбор? – ,ответив на который, вы придете к выводу о том, что каждый из нас сам делает выбор. Свой личный выбор. Мы ответственны за свой выбор, за то, что мы смотрим, читаем, с кем общаемся в реальной жизни и в интернете.

Исходя из этого, какое влияние на нас окажут современные инфокоммуникационные системы, зависит только от нас.

Дети-дошкольники в большей степени зависят от мнения родителей и значимых взрослых. Поэтому в этом возрасте только родители могут контролировать и оценивать, то под какое влияние попадают их дети.

У маленьких детей сформировать правильную систему ценностей достаточно легко, главное, что родители её тоже придерживались. Здесь важен личный пример самих родителей, их положительное мировосприятие.

Это будет первой ступенью к тому, что у подрастающего поколения начнет формироваться критичность мышления, осознанность выбора, дух национального единства.

Взрослея, дети становятся более самостоятельными в своем выборе, у них начинает формироваться собственная система ценностей и интересов. И первую очередь она будет базироваться на том, что родители сформируют у них в дошкольном возрасте.

Переходя в подростковый возраст, ребенок уже пытается максимально стать взрослым и самостоятельным. И именно поэтому, родителям очень важно вовремя стать другом своего ребенка, знать ту «жизнь», в которой он живет, необходимо вместе читать, смотреть фильмы, обсуждать их. Только надо не забывать выполнять главное условие – не критиковать, а высказывать свое мнение, не оскорблять, а стараться понять героев, не читать нотаций, а дать ребенку самому сделать вывод и обсудить его с вами. Общение должно быть как с другом, который чуть младше.

Когда дети вступают в этот возраст, родители начинаю бояться за своих детей, за их безопасность в интернете. В связи с этим, они начинают всячески запрещать им пользоваться, но к сожалению, подобные меры не приводят к желаемому результату, родители рискуют испортить свои отношения с детьми, которые потом будет сложно восстановить.

Здесь очень важна будет работы школы по организации встреч с родителями, на которых им будут объясняться правила безопасного использования сети интернет, о том, что интернет не такое уж зло, как нам иногда кажется.

Очень важно, чтобы мы взрослые поняли, что очень часто сами помогаем современным инфокоммуникационным технологиям оказывать на наше подрастающее поколение негативное и пагубное влияние. Например, мы приходим с работы, включаем телевизор, и начинаем просмотр фильмов и

передач, которые по возрастным ограничениям совершенно не подходят нашим детям. То есть, мы сами осознано, подвергаем своего ребенка негативному влиянию, мы начинаем формировать у него систему ценностей, ту которую, ему покажут в выбранном нами фильме или передаче.

Поэтому, очень важно говорить с родителями о том, чтобы мы общими усилиями оказывали положительное влияние на подрастающее поколение, делали интернет более безопасным, формировали правильные системы ценностей у детей, формировали критичность и избирательность мышления детей, стараться сделать так, что от современных инфокоммуникационных технологий было только позитивное и положительное влияние.

Закончить статью мне хотелось бы словами Джонни Деппа: «Ты – это то, что ты делаешь. Ты – это твой выбор. Тот, в кого себя превратишь».

Ермошин А. В., Чракян К.Г.,

г. Шуя

ИНФОРМАЦИОННЫЕ СИСТЕМЫ ТРУДОУСТРОЙСТВА ВЫПУСКНИКОВ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ

Одним из доминирующих мотивов получения высшего образования является успешное трудоустройство в выбранной специальности. После получения образования перед выпускником стоит проблема трудоустройства. Одна часть выпускников находит работу ещё во время учебы, другая часть «по знакомству» и наконец третья часть, о которой пойдет речь, это категория выпускников, которые нетрудоустроены.

Современные информационные технологии позволяют найти работу в интернете, хоть это и эффективный метод поиска работы, но он имеет много недостатков. Основным недостатком поиска работы в интернете для выпускника является то, что большое количество выпускников не имеет опыта работы. Большинство работодателей не хотят принимать на работу неопытного сотрудника или обучать его. Поэтому самый эффективный способ поиска работы для нетрудоустроенного выпускника – обратится в центр содействия трудоустройству выпускников в вузе, где он проходил обучение. В связи с тем, что работодатель обратившийся в вуз с целью найти работника информирован, что у выпускников отсутствует опыт работы по своей специальности. Такой работодатель готов сам обучить сотрудника.

В современном вузе хранится и обрабатывается огромное количество различных данных, связанных с обеспечением учебного процесса, персональные данные студентов и сотрудников, служебная, коммерческая и иная конфиденциальная информация. Эти данные требуют надежного хранения и защиты информации.

В автоматизированной информационной системе содействия трудоустройству выпускников используется база данных для хранения информации о работодателях и выпускниках. В этой базе хранится большой

массив персональных данных, поэтому система информационной безопасности образовательного учреждения должна обеспечивать целостность баз данных и гарантировать невозможность несанкционированного доступа к ней.

Самые популярные каналы утечки информации характеризуются неумышленным разглашением информации сотрудниками по причине слабой профилактической работы, слабого владения инструкциями по работе с конфиденциальной информацией и неумением определять уровень ее конфиденциальности.

Каналы утечки информации можно разбить на четыре категории [1].

Первая – каналы, которые имеют доступ к элементам системы, но не требуют их изменения. К такой категории относятся устройства перехвата электромагнитных излучений и наводок, подслушивающие устройства и устройства для скрытого видеонаблюдения.

Вторая – каналы, которые имеют доступ как к элементам системы, так и к изменениям структуры их компонентов. К ней относятся наблюдение за информацией в процессе обработки, преднамеренное считывание данных из файлов других пользователей, хищение, копирование и чтение из носителей информации, а также поиск и использование так называемых «лазеек», «дыр» и «люков» для осуществления обхода от ограниченного доступа к информации.

Третья – противозаконное подсоединение особой фиксирующей техники к устройствам системы либо к линиям связи, злоумышленное изменение системы для того чтобы данные совершали сбор и регистрировали защищаемую информацию, выведение из строя механизмов защиты.

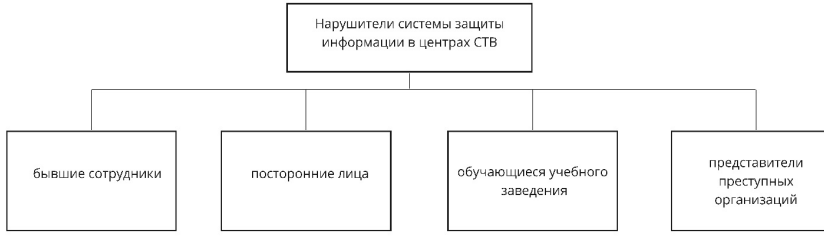
Четвертая – незаконное получение данных посредством подкупа или шантажа должностных лиц соответствующих служб и получение данных посредством подкупа и шантажа работников, либо людей, которые имеют сведения о данной сфере деятельности.

Представленная группировка каналов утечки информации наглядно показывает, то что проблему невозможно решить каким-либо одним методом, тем более решить ее полностью. Помимо этого, осуществление различных мер по ограничению доступа к данным, либо ее распространению снижает

производительность деятельности организации. Разумный подход заключается в сочетании рационального доступа со строгой регламентацией работы с защищёнными данными. В этом случае необходимо создать систему организационно-технических мероприятий, позволяющие перекрыть главные каналы утечки данных с определенной степенью надежности и уменьшить риски без значимого снижения производительности бизнес-процессов.

Значительная часть факторов влияющих на появление возможностей утечки информации в образовательном учреждении, появляется из-за отсутствия нормативной базы, недостаточной квалификацией работников в сфере защиты информации и в отсутствие средств защиты.

Возможными нарушителями системы защиты информации в центрах содействия трудоустройству выпускников могут выступать бывшие сотрудники, посторонние лица, студенты, аспиранты и представители криминальных организации.



Система защиты информации в центрах содействия трудоустройству выпускников имеет ряд недостатков.

Многие предприятия не имеют положения об обработке персональных данных, что не дает возможность регулировать процесс доступа к персональным данным.

У большинства эксплуатируется аналоговая система видеонаблюдения, качество видеосигналов которых не позволяют идентифицировать злоумышленников.

Видеорегистраторы не защищены от возможного воздействия злоумышленников.

Для обеспечения организационной защиты не ведутся журналы паролей и учета доступа к рабочим местам, нет межсетевого экрана, сертифицированного средства контроля и фильтрации сетевого трафика.

С целью улучшения системы защиты информации в центрах СТВ определены следующие направления:

1. Ввод дополнительных мер в политике ИБ образовательного учреждения.

2. Проведение мероприятий, посвященных на соблюдение политик безопасности и инструкций, направленных на защиту информации.

3. Усовершенствование системы видеонаблюдения, посредством внедрения современных AHD- систем видеонаблюдения

В рамках усовершенствования организационной защиты необходимо ведение журналов паролей и учета доступа к рабочим местам, также рекомендуется использовать межсетевой экран и установить сертифицированное средство контроля и фильтрации сетевого трафика. Кроме того, предполагается установка средства защиты информации от несанкционированного доступа совместимого с новейшим программным обеспечением. Дополнительным компонентом эффективности данной системы защиты является создание стандартного положения о защите персональных данных в центре содействия трудоустройству выпускников.

Рекомендованные меры, на наш взгляд, имеют все шансы увеличить безопасность и эффективность системы защиты информации в центрах содействия трудоустройству выпускников при соблюдении норм эксплуатации системы, организационных требований и рекомендации.

Литература:

1. Информационная безопасность государственных организаций и коммерческих фирм / А. В. Волокитин, А. П. Маношкин, А. В. Солдатенков, С. А. Савченко, Ю. А. Петров. – Москва : ФИОРД-ИНФО, 2002. – 272 с.

2. Российская Федерация. Законы. Федеральный закон об информации, информационных технологиях и о защите информации : от 27 июля 2006 г. № 149-ФЗ // Российская газета. – 2006. – 29 июля.

3. Российская Федерация. Законы. Федеральный закон о персональных данных : от 27 июля 2006 г. № 152-ФЗ // Российская газета. – 2006. – 29 июля.

4. Храмов, В. В. Информационная безопасность школы : от защиты информации к безопасности : X Южно-российская межрегиональная научно-практическая конференция «Информационные технологии в образовании». – Ростов : ИТО-РОСТОВ, 2010.

Тельный А.В., Шибнев Е.А.,

г. Владимир

МОДЕЛИ И АЛГОРИТМЫ ОПТИМИЗАЦИИ РАЗМЕЩЕНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ТЕЛЕКОММУНИКАЦИЙ И ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ АНАЛИЗА АРХИТЕКТУРНО-ПЛАНИРОВОЧНЫХ РЕШЕНИЙ ПРОЕКТИРУЕМЫХ ОБЪЕКТОВ

Предметом исследований являются качественные показатели функционирования технических средств защиты информации и защищенность телекоммуникационной среды в зависимости от архитектурно-планировочных решений проектируемых объектов. К научной новизне проводимого исследования можно отнести: формирование новых моделей и алгоритмов качественных характеристик функционирования технических средств защиты информации (ТСЗИ) и телекоммуникационной среды (ТКС) в зависимости от архитектурно-планировочных решений проектируемых объектов. Целями исследования являются: -формирование моделей и алгоритмов качественных характеристик функционирования технических средств защиты информации (ТСЗИ) и телекоммуникационной среды (ТКС) в зависимости от архитектурно-планировочных решений проектируемых объектов, решение задач оптимизации топологии помещений объекта, размещения ТСЗИ и средств телекоммуникаций для повышения качественных показателей их функционирования.

Для достижения целей исследования необходимо решить следующие задачи:

1. Классификация ТКС здания (объекта) и описание требований существующих нормативно-распорядительных документов и стандартов к их размещению;
2. Классификация используемых технических средств охраны (ТСО), средств контроля и управления доступом (СКУД), средств охранного телевидения

(СОТ), технических средств защиты информации от утечки по техническим каналам (ТСЗИ от УТК), элементов инженерно-технического укрепления элементов строительных конструкций (ИТУ) объекта и описание требований существующих нормативно-распорядительных документов и стандартов к их размещению;

3. Анализ требований отдельных ведомственных и вневедомственных документов к проектированию ТСО, СКУД, СОТ, ТСЗИ от УТК, ИТУ особо важных, режимных и выделенных помещений;

4. Осуществить формализацию математического описания архитектурно-планировочных решений проектируемого объекта и инженерных коммуникаций в нем;

5. Анализ качественных показателей функционирования ТКС и ТСЗИ по п.п.1-2 для каждой из подсистем, которые можно выявлять на этапе проектирования объектов и которые зависят от архитектурно-планировочных решений проектируемых объектов;

6. Категорирование по критичности (важности) показателей по п.5;

7. Формализация математического описания размещения средств ТКС и ТСЗИ по п.п.1-2 для каждой из подсистем, при котором показатели их функционирования будут наилучшими;

8. Постановка задач оптимальности топологии размещения ТКС и ТСЗИ по п.п.1-2 для каждой из подсистем на проектируемых объектах с учетом непротиворечивости оптимизационных задач для каждой из подсистем;

9. Математическая формализация правил изменения функционального назначения помещений (экспликации);

10. Математическое описание показателей качества размещения ТКС и ТСЗИ по п.п.1-2 для каждой из подсистем на проектируемых объектах для конкретного варианта экспликации помещений и поставленной оптимизационной задачи;

11. Сравнение вариантов размещения ТКС и ТСЗИ по п.п.1-2 для каждой из подсистем на проектируемых объектах по критериям оптимальности и в

соответствии с экономическими затратами по реализации разных вариантов. Математическое описание выбора варианта;

12. Создание обобщенного алгоритма расчета показателей качества размещения ТКС и ТСЗИ по п.п.1-2 для каждой из подсистем для всех вариантов экспликации помещений и выбора лучшего варианта;

13. Формирование структуры базы знаний по объектам для решения задач оптимизации размещения ТКС и ТСЗИ в зависимости от архитектурно-планировочных решений проектируемых объектов;

14. Апробация полученных моделей и алгоритмов.

Литература:

1. Тельный, А. В. Оценка защищенности информационных ресурсов организации от несанкционированного доступа нарушителей в здания и помещения / А. В. Тельный, Ю. М. Монахов, М. Ю. Монахов // Известия высших учебных заведений. Технология текстильной промышленности. – 2016. – № 5. – С. 259-263.

2. Тельный, А. В. Автоматизация оценки достаточности технических средств охраны и безопасности для защиты от несанкционированного доступа производственного объекта / А. В. Тельный, Ю. М. Монахов, М. Ю. Монахов // Известия высших учебных заведений. Технология текстильной промышленности. – 2016. – № 5. – С. 263-267.

Сведения об авторах

Абрамова Ольга Игоревна, руководитель учебного дела регионального аттестационного центра ООО «Инфоцентр»;

Волчек Виктор Николаевич, инженер-исследователь Института Проблем Информатики Российской Академии Наук (г. Москва);

Ермошин Александр Владимирович, кандидат технических наук, доцент кафедры «Информационных систем и технологий» Шуйского филиала Ивановского государственного университета г. Шуя;

Логинова Наталья Александровна, учитель информатики МБОУ «СОШ №2 г. Суздаля»;

Марцева Алёна Евгеньевна, студент кафедры «Информатика и защита информации» государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» г. Владимир;

Мишин Денис Вячеславович, кандидат технических наук, доцент кафедры «Информатика и защита информации» государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» г. Владимир;

Монахов Михаил Юрьевич, доктор технических наук, профессор кафедры «Информатика и защита информации» государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» г. Владимир;

Монахов Юрий Михайлович, кандидат технических наук, доцент кафедры «Информатика и защита информации» государственного бюджетного образовательного учреждения высшего профессионального образования

«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» г. Владимир;

Порфирьев Артём Андреевич, студент кафедры «Информатика и защита информации» государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» г. Владимир;

Солдатова Галина Уртанбековна, доктор психологических наук, профессор кафедры психологии личности факультета психологии МГУ имени М.В. Ломоносова;

Сорокина Мария Александровна, студент кафедры «Информатика и защита информации» государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» г. Владимир;

Татова Екатерина Дмитриевна, студент кафедры «Информатика и защита информации» государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» г. Владимир;

Тельный Андрей Викторович, кандидат технических наук, доцент кафедры «Информатика и защита информации» государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» г. Владимир;

Теславская Оксана Игоревна, научный сотрудник центра мониторинга рисков и социально-психологической помощи, Академия социального управления; психолог-исследователь Фонд Развития Интернет, г. Москва;

Федорова Екатерина Васильевна, педагог-психолог, социальный педагог МБОУ СОШ №44, г. Владимир;

Харламов Алексей Романович, студент кафедры «Информатика и защита информации» государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» г. Владимир;

Чракян Карен, кандидат технических наук, доцент кафедры «Информационных систем и технологий» Шуйского филиала Ивановского государственного университета г. Шуя;

Шеремет Денис Александрович, студент кафедры «Информатика и защита информации» государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» г. Владимир;

Шибнев Егор Андреевич, студент кафедры «Информатика и защита информации» государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» г. Владимир.

Содержание

Диалог-online

сборник материалов

Подписано в печать 20.09.18.
Формат 60x84/16. Усл. печ. л. 3.50.

Заказ № 1916. Тираж 100 экз.

Издательство Транзит-ИКС
600009, Владимир, ул. Электрозаводская, 2, оф.55