7. Nonaka, I. Perspective — Tacit Knowledge and Knowledge Conversion: Controversy and Advancement in Organizational Knowledge Creation Theory [Text] / I. Nonaka, G. von Krogh // Organization Science. — 2009. — Vol. 20, № 3. — P. 635–652. doi:10.1287/orsc.1080.0412
8. Cohn, D. Business artifacts: A data-centric approach to modeling business operations and processes [Text] / D. Cohn, R. Hull // Bulletin of the IEEE Computer Society Technical Committee on Data Engineering. — 2009. — Vol. 32, № 3. — P. 1–7.
9. Bhattacharya, K. Artifact-centered operational modeling: Lessons from customer engagements [Text] / K. Bhattacharya, N. S. Caswell, S. Kumaran, A. Nigam, F. Y. Wu // IBM Systems Journal. — 2007. — Vol. 46, № 4. — P. 703–721. doi:10.1147/sj.464.0703
10. Görg, C. Visual Representations [Text] / C. Görg, M. Pohl, E. Qeli, K. Xu // Human-Centered Visualization Environments. — Springer Science + Business Media. — P. 163–230. doi:10.1007/978-3-540-71949-6_4
11. Günther, C. W. OpenXES. Developer Guide [Text] / C. W. Günther, E. Verbeek. — Technische Universiteit Eindhoven University of Technology, 2014. — 38 p.
12. Kalynychenko, O. Implementation of search mechanism for implicit dependences in process mining [Electronic resource] / O. Kalynychenko, S. Chalyi, Y. Bodyanskiy, V. Golian, N. Golian // 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS). — Institute of Electrical and Electronics Engineers (IEEE), 2013. — Available at: \www/URL: https://doi.org/10.1109/idaacs.2013.6662657

ВИДІЛЕННЯ КОНТЕКСТНО-ПРОЦЕДУРНИХ ЗАЛЕЖНОСТЕЙ ЗНАННЯ-МІСТКИХ БІЗНЕС-ПРОЦЕСІВ НА ОСНОВІ АНАЛІЗУ ЛОГІВ

Розглянуто знання-місткі бізнес-процеси, які адаптуються виконавцями під час виконання за допомогою персональних знань і досвіду. Показано, що для підвищення ефективності управління такими процесами необхідно виявити контекстно-залежні знання виконавців і потім включити їх в модель процесу. Запропоновано метод виділення контекстно-процедурних залежностей знання-місткого бізнес-процесу на основі аналізу логів.

Ключові слова: знання-місткий бізнес-процес, інтелектуальний аналіз процесів, процесне управління.

Левыкин Виктор Макарович, *доктор технических наук, профессор, кафедра информационных управляющих систем, Харьковский национальный университет радиоэлектроники, Украина,* ***e-mail: levykinvictor@gmail.com****.*
Чалая Оксана Викторовна, *кандидат экономических наук, доцент, кафедра информационных управляющих систем, Харьковский национальный университет радиоэлектроники, Украина,* ***e-mail: oksana.chala@nure.ua****.*

Левикін Віктор Макарович, *доктор технічних наук, професор, кафедра інформаційних управляючих систем, Харківський національний університет радіоелектроніки, Україна.*
Чала Оксана Вікторівна, *кандидат економічних наук, доцент, кафедра інформаційних управляючих систем, Харківський національний університет радіоелектроніки, Україна.*

Levykin Viktor, *Kharkiv National University of Radio Electronics, Ukraine,* ***e-mail: levykinvictor@gmail.com****.*
Chala Oksana, *Kharkiv National University of Radio Electronics, Ukraine,* ***e-mail: oksana.chala@nure.ua***

УДК 614:18:574.2
DOI: 10.15587/2312-8372.2016.86247

Березуцкий В. В.,
Халиль В. В.,
Горбенко В. В.,
Янчик А. Г.,
Макаренко В. В.,
Люфтман Д.

АНАЛИЗ ВЛИЯНИЯ КИБЕРОПАСНОСТИ НА ПРОФЕССИОНАЛЬНУЮ БЕЗОПАСНОСТЬ

Рассмотрены проблемы процесса компьютеризации производств, технологий и жизнедеятельности людей в контексте необходимости и возможности обеспечения кибербезопасности и профессиональной безопасности людей. Показано, что масштабы кибертехнологий вызывают необходимость защищать пользователей от киберугрозы рисков использования компьютеров. Основное внимание обращено на безопасность человека, как главного элемента, определяющего источник угроз и необходимость его защиты.

Ключевые слова: *компьютеризация, кибербезопасность, киберугроза, риск, медиа экология, коммуникации, профессиональная безопасность.*

1. Введение

Распространенная и настойчивая головоломка кибербезопасности остается одним из главных вопросов управления и технологий по всему земному шару, без признаков уменьшения ее важности. На самом деле кибербезопасность остается в списке главных проблем управления и топ-технологий с 1980 г. [1], когда было сделано первое обследование ИТ-тенденций. Проблема безопасности представляется в контексте безопасности предприятия в целом, а также охраны здоровья и безопасности работников. Киберугрозы исходят не только от влияния внешних программных продуктов, а также факторов, влияющих на условия труда и квалификации работников на всех уровнях, в том числе аутсорсинга. Кроме того, соображения безопасности производства, которые не отвечают нормативным требованиям, также могут привести к нарушению на рабочем месте.

ISSN 2226-3780

Актуальность работы определяется тем, что в настоящее время кибероопасность вышла за пределы IT специалистов и ее проблемы стали касаться уровней национальной безопасности. Учитывая масштабы компьютеризации промышленного, банковского и социального секторов экономики, а также распространение компьютеров и компьютерных технологий в обществе, эта проблема разрастается с каждым днем. Доступность, простота и удобство с одной стороны, с другой стороны отодвигают на второй план здоровье и безопасность пользователей и среды обитания человека, что недопустимо. Поэтому необходимо анализировать степень рисков использования кибертехнологий и находить средства и методы обеспечения кибербезопасности.

2. Объект исследования и его технологический аудит

Объектом исследований является система управления профессиональной безопасностью на производстве. Старое название этой системы — система управления охраной труда (СУОТ), но в контексте движения Украины в Европейское содружество и уточнение некоторых понятий, и определений, используемых раннее, уже давно термин «охрана труда» предлагается заменить общепринятым термином — профессиональная безопасность. Профессиональная безопасность определяется множеством составляющих, в том числе и кибербезопасностью, которая может стать причиной несчастного случая или даже аварии (катастрофы) на производстве. Система управления профессиональной безопасностью (СУПБ) является сложной и многоуровневой композицией, функциональность которой зависит от совершенства компьютерных программ и уровня подготовки всего инженерного и руководящего состава предприятия. Для эффективности работы СУПБ должен использоваться аудит профессиональной безопасности, который рассматривает организационные, технические, психофизиологические и другие аспекты трудовой деятельности. СУПБ является составной частью общей системы управления предприятием, которая обеспечивает бесперебойную и эффективную работу самого главного элемента на производстве — человека.

Главным недостатком системы управления профессиональной безопасностью на производстве является непредсказуемость психофизиологического состояния человека, его зависимость от внутренних и внешних факторов, в том числе и от компьютера. Влияние компьютеров на человека, проявляется по многим показателям. В некоторых случаях результат этого воздействия диагностируется медиками как заболевание. Компьютерные технологии быстро продвигаются вперед и далеко не все в Украине пользователи знакомы с технологиями кибербезопасности, и поэтому являются легко уязвимыми к кибератакам. Поэтому обязательным должно быть сейчас введение в компетенции руководителей и инженерно-технических работников всех уровней, занятых в СУПБ, повышение знаний по кибербезопасности и совершенствование системы защиты предприятий от кибератак и других внешних и внутренних влияний, осуществляемых через современные информационные технологии. Методические рекомендации по созданию СУОТ приведены Международной организацией труда (МОП) на их официальном сайте.

3. Цель и задачи исследования

Целью данной работы является исследование устойчивости системы управления профессиональной безопасности к киберугрозам и кибератакам, которые стали главным атрибутом в 21 веке.

Для достижения поставленной цели были сформулированы следующие задачи:

1. Определить масштабы киберугроз в Украине и в мире.
2. Идентифицировать существующие технологии защиты от основных источников кибератаки.
3. Выполнить анализ влияния кибероопасности на профессиональную безопасность и безопасность производств.
4. Проанализировать влияние кибернекомпетентности на безопасность пользователей и окружающей среды.

4. Анализ литературных данных

В настоящее время проблема контроля состояния киберпространства становится на первое место для Украины и мира [1]. Средства и мероприятия по контролю над киберпространством, формируют систему защиты от киберугроз [2]. Развитие информационной среды в 21 веке может быть обеспечено только при надлежащем уровне защиты конфиденциальности, общения с выполнением общепринятых норм и правил поведения пользователей всех уровней. Киберпространство открыто для всех, а это несет угрозы, которые могут привести к тяжелым последствиям. Анализ современной терминологии, применяемой в средствах коммуникаций, показывает их большое разнообразие и появление совершенно новых, таких как медиаэкология [3]. Это свидетельствует о динамизме и популярности развития информационных систем, которое связано с программным обеспечением и начало формировать некую зависимость предпринимателей от разработчиков программ. Сложность процесса разработки программ, применение новых информационных технологий и перспективность развития этого направления, привлекает все больше специалистов, которые большое количество времени проводят с компьютерами и при этом ухудшают состояние своего здоровья. Отсюда появляется связь глобального киберпространства с безопасностью производства и профессиональной безопасностью служащих. На предприятии вопросы профессиональной безопасности должна регулировать системы управления охраной труда, которая является целевой подсистемой безопасности предприятия в целом [4, 5]. Однако изменения в мире в последние десятилетия и появление новых международных стандартов настоятельно требуют пересмотра подходов в этом вопросе. В системе управления охраной труда, как в целом в системе управления предприятием, должны присутствовать элементы кибербезопасности. Киберугрозы можно выявить только, применив методы априорного и апостериорного анализа источников возникновения киберугроз [6]. На основе этих данных была предложена методика определения рисков их реализации, для пользователей компьютеров с разными уровнями подготовки. Наиболее распространенные угрозы для пользователей (программы-вирусы, трояны, программы шпионы и прочие) приведены в достаточном количестве в интернет ресурсах, которые

постоянно обновляются [7, 8]. Доступность киберпространства и рост киберпреступности, как следствие этого, выдвинули понятие кибербезопасности на уровень национальной безопасности в Украине и в мире [9–12]. Во многих странах мира созданы специальные отряды киберполиции, для контроля в киберпространстве. В Украине такое подразделение киберполиции создано в 2015 году. Надо больше заниматься просветительской работой в этом направлении, о чем свидетельствуют опросы [13].

Кибернетика, как наука, открыла путь информационным технологиям, однако в современном виде она предстала как «кибер» [14]. За последние 40 лет число пользователей киберпространства увеличилось до 2,5 млрд и составило 35 % населения нашей планеты [15]. Люди стали больше времени проводить в киберпространстве, подменяя реальный мир виртуальным. В Украине количество пользователей составляет до 43,4 % от общего населения страны. К пользователям компьютеров относятся все категории жителей, в том числе дети и подростки. Негативное влияние киберпространства на здоровье пользователей и население страны становится все активным [16]. Киберугрозы выходят за пределы виртуального пространства и начинают влиять на пользователей на рабочем месте и вне работы. В последнее годы все чаще поднимают вопрос по необходимости обучения населения киберграмотности, что позволит защитить пользователей и среду обитания человека от киберугроз [17].

Новизна постановки проблемы определяется необходимостью изучения влияния киберпространства на профессиональную безопасность и разработки подходов к определению рисков: ухудшения здоровья, возникновения аварийных ситуаций, хищения конфиденциальной информации, нарушения системы управления производством и других.

Отсутствие источников научной периодики по данному вопросу объясняется тем, что очень тяжело напрямую связать влияние кибератаки на физическое состояние работника. Как правило, такое воздействие носит непрямой характер и проявляется в конкретных ситуациях как последствие. Например, нет ни одного сообщения о том, что произошло в Украине во время кибератаки на энергосистемы в 2015 г. на рабочих местах, в лифтах, на рабочих участках, когда отключилась вся электроэнергия. Можно только предположить, что кто-то мог травмироваться, на кого-то могло что-то наехать в темноте, и прочие. Но все это не афишировалось, и информации нет. Только последние статьи и исследования ученых, которые приведены далее в статье, свидетельствуют о наличие физического воздействия киберпространства на людей.

5. Материалы и методы исследований

Для исследований были использованы научные технологии анализа, синтеза, индукции и дедукции, с применением информационных технологий и системного анализа, моделирования и использования теории множеств. Объект исследования представляет собой сложную многоуровневую систему управления безопасностью персонала и производства, с множеством связей. Для анализа надежности такой системы и профессиональной безопасности, использовали теорию рисков.

6. Результаты исследований

6.1. Киберопасность и безопасность производства. Кибербезопасность представляет собой комплекс, включающий в себя: средства, стратегии, принципы обеспечения безопасности, гарантии безопасности, управление рисками, действия, профессиональная подготовка, страхование и технологии, которые используются для защиты киберсреды, ресурсов организаций и пользователей [2].

Сначала появление термина «киберугроза» значило только незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных целей [3]. В настоящее время киберугроза приобрело более широкий масштаб и охватывает все аспекты киберпространства от одиночного пользователя до национальных интересов государств. Это настоятельно требует изменить существующие формулировки и рассматривать проблемы, появившиеся с появлением компьютеров, компьютеризации производств и среды обитания человека, в комплексе сложных существующих и новых факторов, которые являются, с одной стороны, достижением и прогрессом человечества, а с другой стороны несут вред.

Активный рост новых средств коммуникаций вызвал появление новых, совсем необычных выражений, таких, как например медиаэкология или экология средств коммуникации: media ecology (англ.). Под средствами коммуникации имеются в виду любые предметы человеческой культуры, рассматриваемые по отношению к их коммуникативной значимости. Это быстро растущая область исследований, сначала оформившаяся в самостоятельный подход в Канаде и США в конце 1950-х — начале 1960-х годов, а затем распространившаяся во многих других странах. В качестве места появления термина media ecology называют два университета: Торонтский университет (где автором термина считается Маршалл Маклуэн) и Нью-йоркский университет. Экология средств коммуникации возникла на стыке социальной экологии и исследований коммуникационного воздействия предметов культуры (артефактов). В центре внимания экологов средств коммуникации сегодня — всестороннее воздействие электронного коммуникационного окружения на человека и общество [4].

Совершенствуются программные обеспечения и совершенствуются вредоносные программы. Появляются новые и новые разработки, которые включают в себя шпионские программы, программы хакеры и прочие, что заставляет совершенствовать компьютерные знания всех специалистов любого уровня. Становится необходимым повышение знаний в области кибербезопасности руководителей подразделений и предприятий. Безопасность предприятия и лично каждого менеджера становится зависимой от киберпространства.

Насколько опасны кибератаки показывают следующие результаты: с принадлежащего корпорации Sony сервиса Playstation Network были похищены личные данные 77 млн. пользователей. Похищенная информация включала и номера кредитных карт пользователей. Предварительно ущерб от этой атаки оценивают в 1,25 млрд. долларов [5].

Когда в 1988 году произошли первые инциденты в киберпространстве — червь Морриса — один эксперт посчитал, что ущерб от этого составляет от 100 тыс. до 10 млн. долларов [6].

ISSN 2226-3780

В Украине первый в мире факт кибератаки на объекты энергетики зарегистрировали 23 декабря 2015 г. Хакеры готовились к этому с 2014 года, и в конце прошлого года им это удалось, оставив без света более 200 тыс. украинцев. Кибернетическая атака на энергосети Украины произошла 23 декабря 2015 г. на три организации, обеспечивающие энергоснабжение, — «Прикарпатьеоблэнерго», «Киевоблэнерго» и «Черновцыоблэнерго» [7].

Кибератаки крупных организаций на самом деле составляют лишь небольшой процент от общего количества атак, которые происходят каждый год. 71 % взломов баз данных приходится именно на малый бизнес. Направленный фишинг (Spear Phishing) и «Watering Holes» — наиболее распространенные типы атак. В 91 % кибератак фишинг является первой линией атаки. В то время как традиционные фишинг-атаки раскинули широкую сеть, рассылая электронные письма сотням или тысячам адресатов, направленные фишинг-атаки (гарпунный фишинг, Spear Phishing) нацелены на небольшие подгруппы людей, как правило, сотрудников компаний. Для большинства представителей малого и среднего бизнеса взломы несут тяжелые последствия, т. к. большая часть малого и среднего бизнеса попросту не может пережить взлом данных. Взломы могут быть дорогими и, когда база данных не подлежит восстановлению, организации малого и среднего бизнеса сталкиваются не только с репутационными проблемами, но и с операционными — у 68 % предприятий малого и среднего бизнеса в Соединенном Королевстве нет продолжительного бизнес-плана на случай взлома. Потери оказываются настолько значительными, что 60 % вынуждены закрыться в течение 6 месяцев после взлома данных [8].

Киберпреступления по всему миру за 2015 год нанесли ущерб в 158 млрд. дол., передает RNS со ссылкой на отчет по кибербезопасности компании Symantec. По оценке компании, всего жертвами киберпреступлений за прошедший год стали 594 млн. человек. Преступления обошлись в среднем в 358 дол. на человека. Отмечается, что на устранение последствий кибератак в среднем уходил 21 час. Ранее стало известно, что от атак хакеров пострадали The Wall Street Journal, Scottrade и E-Trade [9].

Исследование показало, что компании тратят в среднем 18 дней на ликвидацию последствий нападения. Одна атака обходится в среднем в 416 тыс. дол. Это на 70 процентов больше, чем в 2010 году, когда ликвидация последствий атаки обходилась в 250 тысяч, а работа по устранению последствий занимала не больше 14 дней [10].

Развитие сетевого взаимодействия и появление большого числа потенциально уязвимых устройств с неизбежностью привело к тому моменту, когда кибератаки стали оказывать влияние на реальный мир. Такой вывод содержится в отчете по информационной безопасности за третий квартал 2015 г. «Hazards Ahead: Current Vulnerabilities Prelude Impending Attacks», представленном компанией Trend Micro, мировым разработчиком решений для информационной безопасности. В отчете показано, что прорехи в информационной безопасности и лазейки в мобильных платформах, а также использующие эти уязвимости вредоносные программы подвергают риску уже не только конфиденциальную информацию, но и физическую безопасность, сообщили CNews в Trend Micro. Кроме того, такие пробелы в безопасности подготавливают потенциальную почву для более масштабных событий, которые, по мнению компании, могут произойти в 2016 г.

Киберпреступники использовали украденную информацию для вымогательства и шантажа, что стало настоящей катастрофой как для владельца сайта знакомств компании Avid Life Media, так и для более чем 30 миллионов его пользователей. Сообщалось даже о случаях суицида среди пострадавших из-за последствий, которые оказала эта атака на их личную жизнь [11].

Таким образом, систему, обеспечивающую безопасность производства на современном этапе можно представить в виде кругов Эйлера следующим образом (рис. 1).

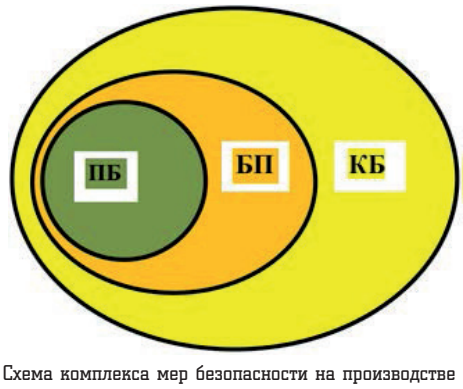

Рис. 1. Схема комплекса мер безопасности на производстве с учетом влияния киберпространства: ПБ — профессиональная безопасность; БП — безопасность предприятия; КБ — кибербезопасность

Отношение включений множеств можно записать ПБ ∈ БП ∈ КБ.

Современная подготовка в высших учебных заведениях не может учесть всех аспектов трудовой деятельности специалистов на производстве. Кроме этого, экономическое состояние государственной системы предполагает многообразие предприятий, организаций и учреждений с различными заданиями и структурой управления. Однако, принимая во внимание важность и тяжесть последствий вредоносного воздействия на работника некоторых программ киберпространства, считаем необходимым ввести обязательное изучение при подготовке специалистов по гражданской защите. А именно по специализации — профессиональная безопасность и здоровье (OSH), которое сейчас называется в Украине — охрана труда, дисциплины кибербезопасность. Специалисты этого профиля, должны заниматься вопросами управления охраной труда на предприятии, как составной частью управления всем производством. В этой системе присутствуют, и используются различные системы контроля над состоянием процессов и рабочих мест, передачи информации, ее обработка и накопление в компьютерных базах данных, и передача данных в руководящие органы и государственные учреждения. При этом используется закрытая для сторонних лиц информация с персональными данными и характеристиками по специалистам, работникам и технологическим процессам, приводятся результаты анализов несчастных случаев и аварий, с указанием слабых сторон производства и прочие, что может быть использовано во вред.

6.2. Система управления предприятием и безопасностью персонала в киберпространстве. Система управления производством (СУП), применяемая на большинстве предприятий стран СНГ, создавалась в условиях изо-

ляции от европейских и других моделей производств. В системе советского периода не было места единой подсистеме обеспечения безопасности производства и персонала. Поэтому подсистема была разрознена и представлена отдельными подразделениями, которые решали вопросы безопасности: экологической, персонала, технической, технологической, экономической и другие.

Современная система управления охраной труда (СУОТ) работников предприятия — это целевая подсистема в системе управления предприятием любой отрасли промышленности [12, 13].

Основные функции системы:

— организация и координация работ по охране труда; планирование работ по охране труда;

— контроль состояния охраны труда и функционирования СУОТ;

— учет, анализ и оценка показателей состояния охраны труда;

— стимулирование за работу по охране труда.

Основные задачи системы:

— обучение работников безопасности труда и пропаганда охраны труда;

— обеспечение безопасности производственного оборудования;

— обеспечение безопасности производственных процессов;

— обеспечение безопасности зданий и сооружений;

— нормализация санитарно-гигиенических условий труда;

— обеспечение работников средствами индивидуальной защиты;

— обеспечение оптимальных режимов труда и отдыха работающих;

— санитарно-бытовое обслуживание работников;

— профессиональный отбор работников по специальностям.

Таким образом, в настоящее время на предприятиях в Украине сложилась ситуация, когда система управления предприятием не имеет целостной системы обеспечения безопасности, отвечающей международным требованиям серии стандартов OHSAS 18000, 27000 и 31000. Требования, предъявляемые к отделам охраны труда в современных условиях, соответствуют международным нормативам. Однако отделы охраны труда не занимались вопросами безопасности производственного оборудования, производственных процессов, обеспечения безопасности зданий и сооружений, особенно в таких объемах, как того требуют указанные международные стандарты. Необходим технологический аудит и постоянный контроль состояния выше перечисленного. В этих условиях обойтись без киберустройств невозможно. Некоторые предприятия уже стали внедрять компьютерные технологии, другие только собираются, но за этим будущее и поэтому им придется столкнуться с проблемой кибербезопасности.

При научном подходе к системному управлению безопасностью производства, появляется набор элементов (компонентов), взаимосвязанных и взаимодействующих между собой так, чтобы могла реализоваться функция системы. Иерархическое представление основано на понятии подсистемы, получаемом при разложении (декомпозиции) системы, обладающей системными свойствами, которые следует отличать от ее элемента — неделимого на более мелкие части (с точки зрения решаемой задачи). Система может быть представлена в виде совокупностей подсистем различных уровней, составляющую системную иерархию, которая замыкается снизу только элементами. Связь является одним из самых уязвимых мест в вопросах кибербезопасности. На рис. 2 показано направление кибератак, которое приводит к нарушению функциональной целостности системы и выход ее из строя.

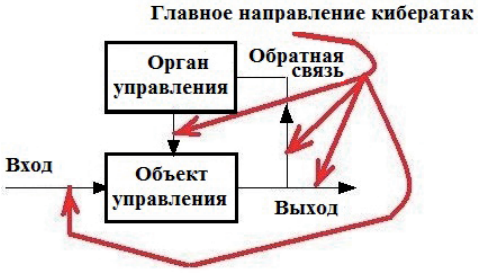

Рис. 2. Пример нарушения связи в системе управления при кибератаке

Поэтому, в системах управления производством и его безопасностью, необходимо предусмотреть технологии защиты от киберугроз и кибератак в киберпространстве.

Все киберугрозы условно можно классифицировать по следующим показателям:

1. По пользователям программами — умение и знание программ, коммутационные, оборудование, персонал.
2. По дислокации — виртуальное и материальное киберпространство.
3. По масштабам — локальные, объектовые, региональные и глобальные.
4. По характеру и цели — экономические, управление, финансовые, террористические, хулиганские и прочие.
5. По человеческому фактору — психофизиологические и эргономические.

6.3. Риск реализации киберугроз. Для определения величины рисков реализация киберугроз необходимо выполнить анализ априорных и апостериорных факторов и источников их возникновения [13].

1. При анализе априорных факторов и источников появления киберугроз по направлению воздействия и источнике необходимо исходить из того, что все программы, которые предназначены для использования в киберпространстве, изначально не несут угрозы для него, а поэтому это можно оценить в балах (0–1) как 0. Однако через какое-то время после их начала применения, эти программы меняют свои показатели, в силу объективных и субъективных условий использования, и поэтому их показатель риска уже возрастает и его показатель риска для киберпространства может возрасти от 0,1 до 0,5 балов. Если эти программы используются в локальной сети (персональный компьютер, без доступа в Интернет) и не имеют возможности внешнего вмешательства, то этот показатель риска не имеет существенного значения, если только программа не предусматривает периодического обновления, а его выполнить нет возможности (разработчики программы прекратили ее сопровождение, сменился собственник и прочие). В Интернете всегда высокий риск киберугроз. Программное обеспечение связано с обновлением его компонентов и подключением к киберпространству. В этом случае есть возможность проникновения в компьютер и взлома пароля, что увеличивает уровень угрозы от 0,5 до 0,9.

ISSN 2226-3780

Не меньшую угрозу несет некомпетентное обслуживание компьютера, а именно — настройка, подключение, обслуживание и т. п. Почему-то принято считать, что за компьютером работают профессионалы, но это не отвечает действительности. А отсюда следует вывод, что необходимо различать IT профессионалов, продвинутых пользователей, обычных пользователей и начинающих пользователей. Каждая из выше названных категорий, вносит свой уровень угрозы в киберпространство своими действиями и активностью. Меньше всего угрозы следует ожидать от IT профессионалов (0 баллов). Далее следует категория продвинутых пользователей, т. е. не имеющих специального IT образования. Эти пользователи изучали основы программирования, знают пакетные программы Word, Excel и другие стандартные программы. В силу необходимости самостоятельно или с помощью кого-то освоили работу на компьютере, изредка обращаясь за советами к профессионалам. Для этой категории степень киберугрозы для киберпространства выше и условно ее можно принять равной 0,1 до 0,3.

Категория обычные пользователи самая распространенная и к ней относятся те, кто не имеет специальных знаний по работе с компьютером или знания на очень малом уровне, отсутствует практический опыт, и они не очень торопятся устранять эти недостатки. Они, как правило, не знают или плохо знают английский язык, а поэтому предупреждения и другие команды, появляющиеся на экране монитора, вызывают у них панику, приводят к ошибкам в управлении, могут даже удалить нужные им программы и информацию. Такая категория специалистов, несет более высокий уровень угроз и ее в баллах условно можно оценить в интервале от 0,4 до 0,7. Категория начинающие пользователи является самой опасной для киберпространства, т. к. они учатся и делают ошибки. Степень угрозы этой категории следует оценить на самом высоком уровне 0,8–0,9. Уровень 1 не следует присваивать никому, т. к. никто из них не делал ошибки специально, т. е. угрозы появились не умышленно. На рис. 3 показана условная шкала рисков киберугроз.

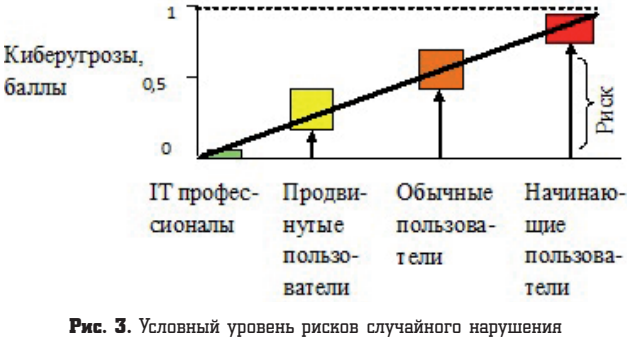

Рис. 3. Условный уровень рисков случайного нарушения кибербезопасности программными пользователями

На украинском сайте Zillya приведена азбука по информационной безопасности, где описываются некоторые программы вирусы и антивирусы [14].

«Дарвин». Компьютерная игра, разработанная тремя инженерами фирмы Bell Telephone Laboratories, в которой программы-«организмы» загружались на компьютеры друзей, копировали себя и уничтожали оппонентов. Победителем становился тот, чья программа сделает больше собственных копий и «инфицирует» больше компьютеров. Эти программы-«организмы» можно считать первыми компьютерными вирусами.

«Зомби»-вирус. Вид компьютерного вируса, который позволяет злоумышленнику управлять компьютером без ведома пользователя, обычно запускается троянской программой. Один из самых сложных «троянов» в истории, который смог превратить в «зомби» четыре миллиона компьютеров, — TDL-4. Его авторы придумали собственную систему кодирования, чтобы защитить связь между вирусом и зараженными компьютерами, что сделало уничтожение вредоносного ПО практически невозможным.

Кейлогер, или клавиатурный шпион. Разновидность программного обеспечения, фиксирующий время, продолжительность, место нажатия клавиш на клавиатуре и клики мышью, которые делает пользователь. Применение кейлоггеров злоумышленниками приводит к краже данных аутентификации пользователя. Эти программы также активно используются правоохранительными органами. Так, например, в 2000 году с помощью клавиатурного шпиона FlashCrest iSpy ФБР рассекретило пароли Никки Скарфо-младшего — члена известного филадельфийского мафиозного клана.

«Письмо счастья», или ILOVEYOU. Один из самых оригинальных вирусов. Пользователю на электронную почту поступало сообщение «I LOVE YOU» с вложенным файлом. После его открытия компьютер получателя начинал посылать огромное количество спама и удалял важные файлы на ПК. В то время (2000 год) «Письмо счастья» инфицировал 10 % всех компьютеров мира.

Моррис Роберт. Автор первого в мире сетевого червя, который парализовал работу шести тысяч компьютеров сети ARPANET — прототипа современного Интернета. Моррис стал первым в мире обвиняемым в кибермошенничестве и основателем нового типа вредоносных программ. Под впечатлением от атаки червя Морриса американская ассоциация компьютерного оборудования начала День защиты информации (30 ноября), который отмечается и сегодня.

2. По дислокации — виртуальное и материальное киберпространство. Киберугрозы определяются факторами, присутствующими в той или другой среде. Виртуальные киберпространство (программное обеспечение компьютера и Интернет) характеризуется наличием вредоносных программ и программ шпионов, которые нацелены на разрушение кибербезопасности и разрушение программного обеспечения пользователя, на копирование и извлечение конфиденциальной информации с целью использования ее во вред пользователя и предприятия. В данной ситуации наибольший риск у тех, кто является носителем такой информации и соответственно, чем меньше такой информации и значимости пользователя и предприятия, тем меньше уровень риска. В современных условиях защита от киберугрозы в киберпространстве, для значимых по важности информации персон, не может гарантировать кибербезопасность на 100 %, т. к. уровень мастерства хакеров также совершенствуется и с каждым годом становиться все более опасным. Материальное киберпространство характеризуется оборудованием и вспомогательными устройствами, или как его еще называют IT специалисты — железо, которые также характеризуется наличием вредных и опасных для пользователя факторов. Среда размещения компьютеров, должна соответствовать нормативам (в Украине — сухие помещения, без по-

вышенной влажности и химической пыли, с наличием вентиляции и прочие). Кибератаки поражают, прежде всего, виртуальное киберпространство, т. е. программы, а через них воздействуют на киберсреду пользователя.

3. Киберугрозы по масштабам: локальные, объектовые, региональные и глобальные, определяются последствиями разрушающего воздействия кибератак. Локальные характеризуются кибератаками на отдельные компьютеры и предприятия. Региональные характеризуются нарушением кибербезопасности регионов и областей. Глобальные киберугрозы имеют, как результат, нарушение нормального функционирования Интернет сетей в масштабах страны или нескольких стран. Расширение киберпространства в глобальных масштабах с одной стороны несет человечеству ускорение прогресса и улучшение условий жизни, а с другой стороны это потенциальная угроза кибератаки, результатом которой может быть жизнь человечества. В этой ситуации менее уязвимыми являются районы, где нет сплошной зависимости от киберпространства, и существует комбинированная система, в которой киберпространство является только вспомогательным и его поражение и разрушение, не оказывает критического влияния на существование людей. Необходимы резервные системы, которые позволяют уменьшать или нейтрализовать кибератаки.

Компания «Лаборатория Касперского» запустила онлайн-сервис, демонстрирующий в режиме реального времени активные киберугрозы. Здесь ведется статистика по срабатыванию почтовых и веб-антивирусов, выявленным уязвимостям и обнаруженным сетевым атакам в данный момент. Пользователь также может узнать, на каком месте рейтинга оказалась та или иная страна из расчета активности киберугроз. Так, первое место прочно занимает Россия, на втором месте Вьетнам, на третьем США, затем следуют Индия и Казахстан. Беларусь оказалась на 39-й позиции. В одной из самых закрытых стран мира, Северной Корее, также замечена вялая активность антивирусного ПО [15].

4. По характеру и цели киберугрозы классифицируются, как экономические, управление, финансовые, террористические, хулиганские и прочие. Это, прежде всего, те сферы человеческой деятельности, на которую направлены кибератаки. Секретарь СНБО Александр Турчинов отметил, что актуализируются и другие киберугрозы, в частности, растет киберпреступность и активизируется кибершпионаж. Турчинов напомнил, что сами эти проблемы призвана решить недавно принятая стратегия кибербезопасности Украины. Национальный координационный центр кибербезопасности должен стать системообразующим элементом всей системы кибербезопасности и киберзащиты Украины. В состав центра вошли представители ключевых государственных органов, которые отвечают за весь спектр вопросов противодействия широкому спектру киберугроз. В сжатые сроки центр должен провести обзор имеющихся сил, средств и возможностей наращивания потенциала реагирования соответствующих государственных органов. Должно быть четко отработан механизм взаимодействия и информационного обмена субъектов кибербезопасности в случае обнаружения кибератаки и киберинцидентов [16].

Работа по повышению уровня кибербезопасности в Украине пока в самом начале:

— 15 марта 2016 г. указом президента № 96 утверждена Стратегия кибербезопасности Украины;

— 7 июня 2016 г. президент указом № 242 утвердил положение о Национальном координационном центре кибербезопасности, который является рабочим органом СНБО;

— 24 июня 2016 г. Кабинет Министров Украины распоряжением № 440-р утвердил План мероприятий на 2016 г. по реализации Стратегии кибербезопасности.

В рекомендации ТХ1205 Международного союза электросвязи (ITU) записано:

— «Кибербезопасность — это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Общие задачи обеспечения безопасности включают следующее: доступность; целостность, которая может включать аутентичность и безотказность; конфиденциальность».

— Кибербезопасность охватывает не только информацию как объект защиты и технические средства, которые определяют возможности функционирования информации, но и защиту способов функционирования всего киберпространства. Защищается деятельность людей, которая осуществляется с помощью информации, распространяемой посредством технической инфраструктуры.

— Национальные стратегии кибербезопасности появились сравнительно недавно. В США — в 2003 г, во Франции — в 2011 г., а единая стратегия для Евросоюза — только в 2013 г. В 2011 г. в США была принята «Международная стратегия по действиям в киберпространстве». В ней компьютерные атаки приравниваются к форме военных действий, что дает право применять в ответ любое оружие [17].

Уже много лет Украина является страной, в которой активно распространяются компьютерные технологии, но только с осени 2015 года правоохранительные органы МВД приняли решение по созданию подразделения киберполиции. Это подразделение будет заниматься противодействием киберпреступности, расследованием преступлений в сфере использования электронных платежных систем, таких как скимминг (незаконное копирование содержимого треков магнитной полосы или чипов банковских карт); кэш-треппинг (похищение наличности из банкомата путем установки на шатер банкомата специальной удерживающей накладки), кардинг (незаконные финансовые операции с использованием платежной карточки), несанкционированное списание средств с банковских счетов с помощью систем дистанционного банковского обслуживания. Ведомство киберполиции будет вести расследования в сфере фишинга, онлайн-мошенничества, интернет-пиратства в сфере интеллектуальной собственности, противодействие применению методик социальной инженерии, созданию и распространению вирусов и вредоносного программного обеспечения [18].

Киберпреступность составляет 23 % из всех случаев мошенничества в мире, в Украине этот показатель равен 17 %. Киберпреступники совершенствуют свое мастерство и в этом им помогают различные учебные заведения и курсы, которые очень распространены в мире. Отсюда, киберпреступления становятся более изощренными, что намного усложняет борьбу с ними, а также их обнаружение и предотвращение. Принимая во внимание

активный рост пользователей компьютеров и масштабы компьютеризации, следует вывод, что это может привести к большим убыткам и потерям в будущем не только на производстве и отдельных объектах, но в государственных масштабах. Опрос, проведенный в Украине, показал, что 36 % респондентов считают киберпреступность внешней угрозой, 24 % — внутренней, а 34 % респондента относят киберугрозу к обоим вариантам [19].

6.4. Профессиональная безопасность и здоровье при работе и применении киберпространств. Рассмотрим значение слова «кибер». В современном варианте предлагаемом Интернетом, это слово означает: клавиатура на компьютере (от англ. keyboard); «кибер» — кибернетическая машина, компьютер и прочие. Существует еще понятие наука кибернетика, которая произошла от слова kybernaō (греческое слово), что означает управляю, то есть наука об управлении, связи и переработке информации [20]. Именно наука кибернетика стала тем, что сейчас называют «кибер», однако в новом качестве этого слова, сложный математический аппарат, который использовался в кибернетике, требовал и применения специальных машинных технологий для переработки большого объема информации. Применяемые в 70-х годах, электронные машины были громоздки, и тогда никто не мог себе представить, что через 30–40 лет, размеры этих машин уменьшаться в десятки и сотни раз, а проблемы, «сидящие» в них, увеличатся в тысячи раз, и станут угрозой для людей. Появится новое выражение — киберопасность. Исходя из этого, необходимо вспомнить о кибернетике, науке рассматривающей вопросы выбора и проектирование различных устройств и аппаратов, науку, изучающую надежность технических систем и оптимизирующую многочисленные решения с целью получения заданных показателей. Современное понятие «кибер» сильно отличается от науки кибернетики и сильно упрощено с одной стороны. С другой стороны, это понятие включает в себя целый мир, созданный благодаря успехам ученых, в котором присутствует и кибернетика, и много еще нового, что появилось за эти 30–40 лет.

Общее количество пользователей на планете приблизительно около 2,5 млрд, что составляет около 35 % населения нашей планеты [21]. Но процесс этот динамичный и точное число установить практически невозможно.

Последние 10 лет наблюдается значительный рост количества персональных компьютеров. Причин этому много, а именно: рост благосостояния населения многих стран; снижение стоимости компьютеров; развитие науки и новые беспроводные технологии; большое количество студенческой молодежи, использующей компьютеры (обучение, развлечение и общение); доступный Интернет и его технологии; социальные сети и различные сервисы; упрощение денежных переводов и приобретение товаров, и прочие. Люди стали много времени проводить за компьютерами и появилось новое понятие — виртуальный мир, которое еще называют киберпространство. Это мир, в котором математические формулы и компьютерные технологии представлены в псевдо реальном мире, который начинают воспринимать, как существующий, что-то похожее на зазеркалье в сказке «Алиса в стране чудес». Этот «мир» начинает проникать в разум людей и формировать у них определенное мышление и новые подходы к жизни. Для некоторых, реальный мир перестает существовать, так человек не может в нем управлять событиями, а в киберпространстве он герой и тот мир ему становится ближе. Это вызывает психические отклонения и люди становятся зависимыми от виртуального мира, хотя и не подозревают, что там тоже есть свои законы, и там также присутствуют опасности, которые могут разрушить их киберпокой.

Количество пользователей компьютеров, которые потенциально находятся в киберпространстве и часть населения в процентах, сильно отличаются, особенно в небольших странах. Менее 1 % пользователи составляют в странах Нигер (0,83), Гвинея (0,96 %), Восточный Тимор (0,21 %) [14]. Исходя из величины опасности распространения киберугроз, ТОП 10 позиций занимают:

1. Фолклендские острова (95,84 %), Исландия (95 %).
2. Норвегия (93,39 %).
3. Нидерланды (90,72 %), Люксембург (90,62 %), Швеция (90 %).
4. Дания (88,72 %).
5. Финляндия (86,89 %).
6. Великобритания (85 %).
7. Бермуды (84,21 %).
8. Швейцария (83,9 %), Республика Корея (83,7 %), Германия (83 %), Новая Зеландия (83 %).
9. США (81,1 %), Канада (81,6 %), Андорра (81 %).
10. Антигуа и Барбуда (80 %), Лихтенштейн (80 %), Монако (80 %).

В Украине около 19 млн. пользователей, что соответствует 43,4 % от общего населения страны. Какую часть от количества всех пользователей занимают страны, представлено на диаграмме (рис. 4). Украина относится к числу стран с процентным соотношением 30–50 % от всего населения. Эта категория наиболее распространенная в мире.

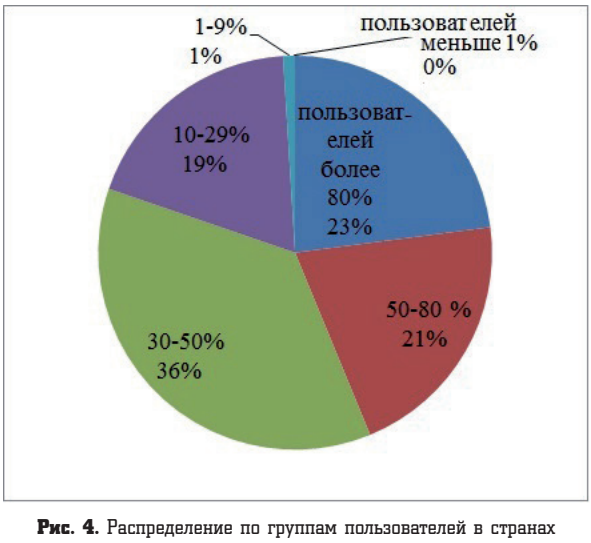

Рис. 4. Распределение по группам пользователей в странах в процентном соотношении к общему количеству пользователей в мире (в процентах)

На рис. 5 показано численное соотношение по категориям пользователей распределенных в процентном отношении по числу пользователей в стране к общему количеству населения.

При работе пользователей и специалистов компьютерных технологий, всегда присутствует набор вредных и опасных факторов, негативно влияющих на состояние здоровья человека. Поэтому существует набор требований и норм, регулирующих работу пользователя ком-

пьютера [22]. Влияние компьютера на здоровье человека характеризуется:

— постоянным сидячим положением;
— большим зрительным напряжением;
— однообразными повторяющимися нагрузками на руки;
— а также нервно-эмоциональным напряжением, связанным с влиянием компьютера на психику человека.

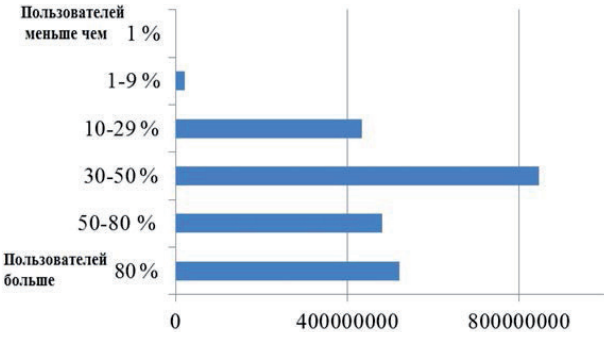

Рис. 5. Количество пользователей в категориях пользователей в процентном отношении к числу населения страны или района земного шара

Опасность компьютера для здоровья проявляется в том, что воздействие перечисленных проблем на здоровье человека проявляется далеко не сразу, а лишь спустя какое-то время. Основные факторы, оказывающие влияние на здоровье человека при работе за компьютером:

— мерцание монитора (влияет на глаза);
— электромагнитное излучение;
— шум (раздражает);
— воздействие на психику;
— стесненная поза (действует на позвоночник);
— микроклимат помещения (влажность, запыленность);
— режим работы (необходимые перерывы на отдых).

Ранее основным источником излучения в персональном компьютере были мониторы с электронно-лучевой трубкой, которые в настоящее время выходят из употребления. Современные жидкокристаллические мониторы в плане излучения считаются намного более безопасными.

Для профилактики органов дыхания необходимо проветривать помещение, где работает компьютер, несколько раз в день, и проводить влажную уборку. Желательно пользоваться ионизатором (например, люстра Чижевского).

Для увеличения влажности можно ставить открытую емкость с водой. Это может быть аквариум с рыбками (увеличивает влажность, а рыбки успокаивают нервы), декоративный водопад (опять же, повышает влажность, а льющаяся вода выполняет функции ионизатора).

Более сложным является вопрос, связанный с заболеваниями мышц и суставов. Однообразное сидячее положение способствует онемению шеи, боли в плечах и пояснице, покалыванию в ногах. Люди, профессионально работающие за компьютером, так же, как и те, у кого сидячая работа, страдают изменениями формы позвоночника и общей мышечной слабостью. Необходимо вести здоровый и активный образ жизни (рис. 6).

Использование мыши небезопасно для здоровья, а точнее, для кисти, запястья, предплечья, плеча. Самым распространенным заболеванием, связанным с использованием клавиатуры и мыши, является синдром запястного канала или туннельный синдром [22].

Рис. 6. Основные направления «кибератак» от киберпространства для пользователя

Для профилактики рук рекомендуется делать перерывы в работе и гимнастику. Также для профилактики предпочтительно использовать удобную выпуклость для запястья. Это может быть соответствующий коврик для мыши, клавиатура специальной формы или «ортопедический» компьютерный стол с необходимыми выпуклостями.

По нормам общая площадь, необходимая для одного взрослого пользователя, составляет не менее 6 кв. м.

Следовательно, киберпространство небезопасно для пользователя и «атакует» его постоянно, с первого контакта с ним, что проявляется в последствие. Пока человек может использовать эффективно только триаду защиты: расстоянием, временем и мощностью источника излучения негативного фактора. Должны быть специальные программы, которые должны отслеживать все эти факторы воздействия и предупреждать пользователя о необходимости сделать перерыв в работе, на какое-то время покинуть свое рабочее пространство. Пользователь должен побеспокоиться о том, чтобы источник генерации вредного энергетического воздействия (ЭМП, шума, вибрации и т. п.) был удален подальше или заменен на другое устройство с меньшим показателем по мощности излучения. Опыт использования подобных программ показывает, что срабатывает человеческий фактор, и работа таких программ сводится к нулю. По нашей просьбе была разработана компьютерная программа, которая запускалась при автозагрузке компьютера и через определенные отрезки времени, появлялись на экране напоминания о вредностях при работе с ПЕОМ и рекомендациях, о том что необходимо сделать перерыв или другие рекомендации, в том числе упражнения для глаз. Пользователи ПЕОМ, вместо того чтобы следовать рекомендациям программы, стали стараться найти выход как их обойти, т. е. найти, как ее отключить или блокировать.

Опасность это негативное свойство системы «человек-среда обитания», способное проявить себя при определенных условиях, причинить ущерб здоровью людей или окружающей среде, и обусловленное энергетическим состоянием среды и действиями человека. Опасность реализуется посредством опасных или

ISSN 2226-3780

негативных факторов, воздействие которых на человека приводит к травме или летальному исходу (поражение электрическим током, наезд автотранспорта, отравление сильными ядами и др.). Но в чем опасность киберпространства для человека?

Людей и живые организмы в жизненном их цикле постоянно сопровождают факторы, которые при определенных условиях оказывают отрицательное воздействие. В зависимости от уровня и продолжительности воздействия вредный фактор может стать опасным. В этом случае следует привести формулировку понятия фактор риска (Фр) — фактор или условие среды обитания, сопутствующий не до конца осознанному (осознанному) действию живых организмов (человека), которое приводит или может привести, к их заболеванию или гибели (например: курение — рак легких, инфаркт миокарда; полет на самолете (осознанная необходимость) — падение с высоты). Можно ли сравнить работу пользователя компьютера с фактором риска? Пользователь находится в опасном киберпространстве, т. е. в опасной зоне. Опасная зона — пространство среды обитания, в котором возможно действие на человека опасного и (или) вредного факторов среды обитания.

По характеру воздействия на человека опасности киберпространства можно разделить на активные и пассивные. К пассивным опасностям относятся такие, которые активизирующиеся за счет энергии, носителем которой является сам человек. Активные опасности — все остальные, проявляющие активность в воздействие на человека. Таким образом, такие опасности как нервно-психические перегрузки, которые подразделяются на умственное перенапряжение; перенапряжение анализаторов; монотонность труда; эмоциональная перегрузка необходимо отнести к пассивным опасностям киберпространства.

С точки зрения психологии, каждый из людей ведет себя так, чтобы как можно меньше у него было проблем, а тем более связанных с болевым ощущением. «Природой» предусмотрено, что боль — это сигнал о каком-либо неблагоприятном для организма человека влиянии или воздействии факторов среды обитания и, соответственно, изменение в неблагоприятную сторону, функциональных параметров, обеспечивающих жизнедеятельность. А какой сигнал должен предупредить пользователя в киберпространстве о превышении допустимого порога и нарушении жизнедеятельности организма? К сожалению, опасности киберпространства не всегда себя проявляют сразу, чаще всего это скрытые отклонения в состоянии здоровья, которые затем переходят в хронические заболевания. Следовательно, все пользователи компьютеров и имеющие отношение к работе в киберпространстве, должны периодически проверять состояние своего здоровья в лечебных учреждениях.

Человек, работающий на предприятии или проживающий в местности, которая при аварии может оказаться в зоне разрушения или воздействия опасностей, подвергается риску. Концепция «индивидуального риска» относится к числу людей, проживающих (работающих) в такой местности и подвергающихся действию опасности. Такие люди называются «рискующими». Пользователи компьютеров также необходимо отнести к такой категории. Сколько таких людей проживающих на Украине можно отнести к этой категории? Это миллионы украинцев, учитываю уровень компьютеризации страны. Риск для определенного человека зависит от целого ряда факторов, зависящих от его места нахождения и времени. Подавляющее большинство людей изменяют свое местонахождение в течение дня и каждый день только определенное время проводят дома. Пользователи компьютеров практически привязаны к одному месту, а следовательно степень риска в большей степени у них будет определяться временем пребывания в киберпространстве.

Специалисты информационной безопасности знают, что самое слабое звено в системе защиты есть сам пользователь. Поэтому, чем больше он будет знать информации об киберугрозах, тем лучше он осознает риски проникновения, что обеспечивает вероятность взлома его компьютера и хищения информации. Исходя из выше сказанного, следует необходимость проведению мероприятий по обучению населения, как пользователей киберпространства, киберграмотности в Украине. Очень важным является наличие инициативы у самих пользователей, и в первую очередь у представителей бизнеса и обычных граждан [23].

7. SWOT-анализ результатов исследования

К достоинствам выполненного исследования следует отнести высветленные проблемы киберопасности, их масштабы и тенденция к их увеличению. Также достоинством является применение классификации пользователей по группам рисков и обработка статистических данных по группам пользователей к населению в разных странах. Выполненный анализ показал, возрастающую зависимость развитых государств от киберпространства, его состояния и уязвимости от хакерских кибератак. Полезной является информация о функциональном влиянии состояния виртуального киберпространства на кибербезопасность производств и профессиональную безопасность работников и служащих.

Выполненный анализ необходимо использовать для повышения компьютерной грамотности пользователей всех уровней, совершенствования методов диагностики киберугрози выявления узких мест в системе управления производством.

Предполагается продолжение исследований совместно с профессионалами, занимающимися обучением по кибербезопасности Украины и GIIM США, Нью-Йорк.

К слабым сторонам исследования следует отнести отсутствие доступной базы данных в Украине и за ее пределами, по исследованию влияния кибератак и киберпространства на физическом уровне на пользователей. Например, сколько человек пострадало при отключении системы подачи воды или электричества, упали с высоты, остановки метро в туннели под землей и т. п.

Отрицательным моментом таких исследований является еще недостаточно развитый уровень компьютеризации в Украине технологий и социальной сферы. Украина только приблизилась к этому порогу и поэтому надо сделать все для изучения последствий и предупреждения нежелательных результатов. Необходимо изучить положительный и негативный опыт в странах, где уровень компьютеризации составляет до 90 %.

8. Выводы

1. Определен масштаб киберугроз в Украине и в мире. В настоящее время киберопасность вышла за пределы IT специалистов и ее проблемы стали касаться уровней национальной безопасности. Про кибератаки и кибер-

угрозы ведут переговоры руководители государств, и принимают национальные программы по защите киберпространства и пользователей во всех странах мира. Проблемы применения компьютеров в повседневной жизни людей, заставляют все настоятельнее требовать обучения пользователей не только как применять программы, но и как сберечь при этом свое и здоровье детей от негативного влияния компьютеров. Это должны знать все и поэтому необходимо больше научных исследований в области киберпространства и защиты его от кибератаки других сопутствующих негативных факторов.

2. Идентифицировано существующие технологии защиты от основных источников кибератаки — технические, организационные, психофизиологические. Кибербезопасность, как обеспечение безопасности предприятия и персонала, является неотъемлемой составляющей успешной работы предприятия в современном мире.

3. Выполнен анализ влияния киберопасности на профессиональную безопасность и безопасность производств. Там, где применяются компьютерные технологии, всегда присутствуют вредные и опасные факторы, сопровождающие компьютеры, как устройства, и влияющие на психофизиологические показатели организма человека, как энергоинформационные источники. Специалисты по вопросам профессиональной безопасности и здоровья персонала должны владеть методами защиты киберпространства предприятия и отдельных подразделений.

4. Проанализировано влияние кибернекомпетентности на безопасность пользователей и окружающей среды. Как показано в исследованиях, одно неосторожное обращение с полученным из киберпространства сообщения, может открыть хакеру путь во всю компьютерную систему предприятия, результатом чего может быть прекращение работы всего производства. Кибербезопасность необходимо рассматривать, как обязательную профессиональную компетентность руководителей подразделений и учитывать при проведении их аттестации.

Литература

1. Luftman, J. Influential IT management trends: an international study [Text] / J. Luftman, B. Derksen, R. Dwivedi, M. Santana, H. S. Zadeh, E. Rigoni // Journal of Information Technology. — 2015. — Vol. 30, № 3. — P. 293–305. doi:10.1057/jit.2015.18
2. Кибербезопасность [Электронный ресурс] // SecurityLab.ru. — Режим доступа: \www/URL: http://www.securitylab.ru/news/tags/%EA%E8%E1%E5%F0%E1%E5%E7%EE%EF%E0%F1%ED%EE%F1%F2%FC/
3. Уильямс, Б. Киберпространство: что это, где это и кому оно надо? [Электронный ресурс] / Б. Уильямс // Belarus Security Blog. — 08.07.2014. — Режим доступа: \www/URL: http://www.bsblog.info/kiberprostranstvo-chto-eto-gde-eto-i-komu-ono-nado/
4. Медиаэкология [Электронный ресурс] // Википедия. — 21.06.2016. — Режим доступа: \www/URL: https://ru.wikipedia.org/wiki/Медиаэкология
5. Кибератаки — понятие, цели, последствия и меры противодействия [Электронный ресурс] // xBB.uz. — 10.01.2014. — Режим доступа: \www/URL: http://xbb.uz/IT/Kiberataki-ponjatie-celi-posledstvija-i-mery-protivodejstvija
6. Кибернетические нападения: какой вред могут они причинить нам? [Электронный ресурс] // Вестник НАТО. — 2013. — Режим доступа: \www/URL: http://www.nato.int/docu/review/2013/Cyber/Cyber-attack-hurt/RU/index.htm
7. Краминская, М. Причины и последствия первой кибератаки на энергосети [Электронный ресурс] / М. Краминская // Информационное агентство «Украинские Национальные Новости». — 04.03.2016. — Режим доступа: \www/URL: http://www.unn.com.ua/ru/news/1552848-prichini-i-naslidki-pershoyi-kiberataki-na-energomerezhi
8. Сивенюк, А. Последствия кибератак для малого и среднего бизнеса [Электронный ресурс] / А. Сивенюк // hi-Tech.ua. — 28.10.2015. — Режим доступа: \www/URL: http://hi-tech.ua/blog/posledstviya-kiberatak-dlya-malogo-i-srednego-biznesa/
9. Потери от кибератак в 2015 году составили $158 млрд [Электронный ресурс] // АО «Газета.Ру». — 24.01.2016. — Режим доступа: \www/URL: https://www.gazeta.ru/tech/news/2016/01/24/n_8160947.shtml
10. Сокуренко, Э. Последствия кибератак обходятся все дороже [Электронный ресурс] / Э. Сокуренко // TechDaily.ru. — 2011. — Режим доступа: \www/URL: http://techdaily.ru/kiberataki-obxodyatsya-vse-dorozhe/
11. Кибератаки стали оказывать влияние на реальную жизнь людей и организаций [Электронный ресурс] // Internetua. — 21.11.2015. — Режим доступа: \www/URL: http://internetua.com/kiberataki-stali-okazivat-vliyanie-na-realnuua-jizn-luadei-i-organizacii
12. Березуцький, В. В. Вступ до спеціальності. Текст лекцій для студентів за напрямком підготовки 6.170202 — Охорона праці [Текст] / В. В. Березуцький. — Х.: Щедра садиба плюс, 2014. — 208 с.
13. Березуцкий, В. В. Производственный риск и человеческий фактор [Текст] / В. В. Березуцкий, И. В. Березуцкий // Матеріали IV науково-практичної конференції «Безпека життя і діяльності людини-освіта, наука, практика». — К.: НАУ, 2005. — 288 с.
14. Сыч, О. Азбука информационной безопасности от А до Я [Электронный ресурс] / под ред. О. Сыч // Zillya! Антивірус. — 12.11.2014. — Режим доступа: \www/URL: http://zillya.ua/ru/azbuka-informatsionnoi-bezopasnosti-ot-do-z
15. Альшевский, Я. В интернете появилась интерактивная карта киберугроз [Электронный ресурс] / Я. Альшевский // Onliner.by. — 28.03.2014. — Режим доступа: \www/URL: https://tech.onliner.by/2014/03/28/cybertreat-2
16. Элементы «гибридной» войны: Турчинов рассказал о киберугрозах со стороны России [Электронный ресурс] // Обозреватель. — 11.06.2016. — Режим доступа: \www/URL: http://obozrevatel.com/crime/41809-elementyi-gibridnoj-vojnyi-turchinov-rasskazal-o-kiberugrozah-so-storonyi-rossii.htm
17. Гусев, С. Как в Украине защищают Интернет: стратегия кибербезопасности [Электронный ресурс] / С. Гусев // Сегодня.ua. — 18.07.2016. — Режим доступа: \www/URL: http://www.segodnya.ua/politics/power/kak-v-ukraine-zashchishchayut-internet-strategiya-kiberbezopasnosti-734330.html
18. Дробаха, А. Чем занимается киберполиция в Украине и других странах мира [Электронный ресурс] / А. Дробаха // Обозреватель. — 15.08.2016. — Режим доступа: \www/URL: http://obozrevatel.com/blogs/63947-chem-zanimaetsya-kiberpolitsiya-v-ukraine-i-drugih-stranah-mira.htm
19. Киберпреступность в Украине [Электронный ресурс] // Информационная корпоративная служба. — 24.12.2011. — Режим доступа: \www/URL: http://z-filez.info/news/kiberprestupnost-v-ukraine
20. Ишлинский, А. Ю. Политехнический словарь [Текст] / под ред. А. Ю. Ишлинского. — 3-е изд. — М.: Советская энциклопедия, 1989. — 656 с.
21. Список стран по числу пользователей интернета [Электронный ресурс] // Википедия. — 05.10.2016. — Режим доступа: \www/URL: https://ru.wikipedia.org/wiki/Список_стран_по_числу_пользователей_Интернета
22. Березуцький, В. В. Основи охорони праці [Текст]: навч. посіб. / В. В. Березуцький, Т. С. Бондаренко, Г. Г. Валенко; за ред. В. В. Березуцького. — 2-е вид., перер. і допов. — Х.: Факт, 2008. — 480 с.
23. Дробаха, А. Спасение утопающих: что украинцы знают о кибербезопасности интернета [Электронный ресурс] / А. Дробаха // Обозреватель. — 13.06.2016. — Режим доступа: \www/URL: http://obozrevatel.com/blogs/60381-spasenie-utopayuschih-chto-ukraintsyi-znayut-o-kiberbezopasnosti.htm

АНАЛІЗ ВПЛИВУ КІБЕРНЕБЕЗПЕКИ НА ПРОФЕСІЙНУ БЕЗПЕКУ

Розглянуті проблеми процесу комп'ютеризації виробництв, технологій та життєдіяльності людей в контексті необхідності і можливості забезпечення кібербезпеки і професійної безпеки людей. Показано, що масштаби кібертехнологій викликають необхідність захищати користувачів від кіберзагроз і ризиків

ISSN 2226-3780

використання комп'ютерів. Основна увага звернена на безпеку людини, як головного елемента, що визначає джерело загроз і необхідність його захисту.

Ключові слова: комп'ютеризація, кібербезпека, кіберзагроза, ризик, медіа екологія, комунікації, професійна безпека.

Березуцкий Вячеслав Владимирович, *доктор технических наук, профессор, заведующий кафедрой охраны труда и окружающей среды, Национальный технический университет «Харьковский политехнический институт», Украина,*
e-mail: qwer@kpi.kharkov.ua*.*
Халиль Виктория Вячеславовна, *ассистент, кафедра охраны труда и безопасности жизнедеятельности, Харьковский национальный университет городского хозяйства им. А. Н. Бекетова, Украина.*
Горбенко Вероника Владимировна, *кандидат технических наук, профессор, кафедра охраны труда и окружающей среды, Национальный технический университет «Харьковский политехнический институт», Украина.*
Янчик Александр Григорьевич, *кандидат технических наук, доцент, кафедра охраны труда и окружающей среды, Национальный технический университет «Харьковский политехнический институт», Украина.*
Макаренко Виктория Васильевна, *старший преподаватель, кафедра охраны труда и окружающей среды, Национальный технический университет «Харьковский политехнический институт», Украина.*
Люфтман Джерри, *кандидат технических наук, профессор, генеральный директор, Глобальный институт управления информационными технологиями, Нью-Джерси, США.*

Березуцький Вячеслав Володимирович, *доктор технічних наук, професор, завідувач кафедри охорони праці та навколишнього середовища, Національний технічний університет «Харківський політехнічний інститут», Україна.*
Халіль Вікторія В'ячеславівна, *асистент, кафедра охорони праці та безпеки життєдіяльності, Харківський національний університет міського господарства ім. О. М. Бекетова, Україна.*
Горбенко Вероніка Володимирівна, *кандидат технічних наук, професор кафедри, кафедра охорони праці та навколишнього середовища, Національний технічний університет «Харківський політехнічний інститут», Україна.*
Янчик Олександр Григорович, *кандидат технічних наук, доцент, кафедра охорони праці та навколишнього середовища, Національний технічний університет «Харківський політехнічний інститут», Україна.*
Макаренко Вікторія Василівна, *старший викладач, кафедра охорони праці та навколишнього середовища, Національний технічний університет «Харківський політехнічний інститут», Україна.*
Люфтман Джеррі, *кандидат технічних наук, професор, генеральний директор, Глобальний інститут управління інформаційними технологіями, Нью-Джерсі, США.*

Berezutskyi Viacheslav, *National Technical University «Kharkiv Polytechnic Institute», Ukraine,* ***e-mail: qwer@kpi.kharkov.ua****.*
Khalil Viktoriya, *O. M. Beketov National University of Urban Economy in Kharkiv, Ukraine.*
Gorbenko Veronica, *National Technical University «Kharkiv Polytechnic Institute», Ukraine.*
Yanchik Alexander, *National Technical University «Kharkiv Polytechnic Institute», Ukraine.*
Makarenko Victoria, *National Technical University «Kharkiv Polytechnic Institute», Ukraine.*
Luftman Jerry, *Global Institute for IT Management, New Jersey, USA*

УДК 519.7:619
DOI: 10.15587/2312-8372.2016.86295

Высоцкая Е. В.,
Панферова И. Ю.,
Коваль С. Н.,
Печерская А. И.,
Абрамова А. А.

РАЗРАБОТКА ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ ОПРЕДЕЛЕНИЯ СЕРДЕЧНО-СОСУДИСТОГО РИСКА У ПАЦИЕНТОВ С НАРУШЕНИЕМ ФУНКЦИИ ПОЧЕК

Построены контекстная диаграмма и диаграмма декомпозиции первого уровня информационной технологии определения сердечно-сосудистого риска у пациентов с нарушением функции почек, которые описывают вход, выход, управляющие воздействия, функциональные информационные процессы, накопители данных, внешние сущности и движение потоков данных между ними. Построена информационно-логическая модель данных, отражающая все объекты и события, информацию о которых необходимо хранить, и связи между ними.

Ключевые слова: *ER-модель, информационная технология, контекстная диаграмма, сердечно-сосудистый риск.*

1. Введение

В течение последних десятилетий в мире наблюдается повсеместный неуклонный рост числа пациентов с нарушением функции почек. Это делает проблему лечения нефрологической патологии одной из центральных в современной нефрологии. Значительный прогресс заместительной почечной терапии, научно-технические достижения в области гемодиализа, широкое внедрение в клинику перитонеального диализа и трансплантации почки создали реальные предпосылки для успешного решения этой проблемы.

Однако, если диагностика и лечение нарушения функции почек достаточно хорошо разработаны, то при ведении пациентов с сочетанной патологией часто возникают трудности. Особое место среди сочетанных

