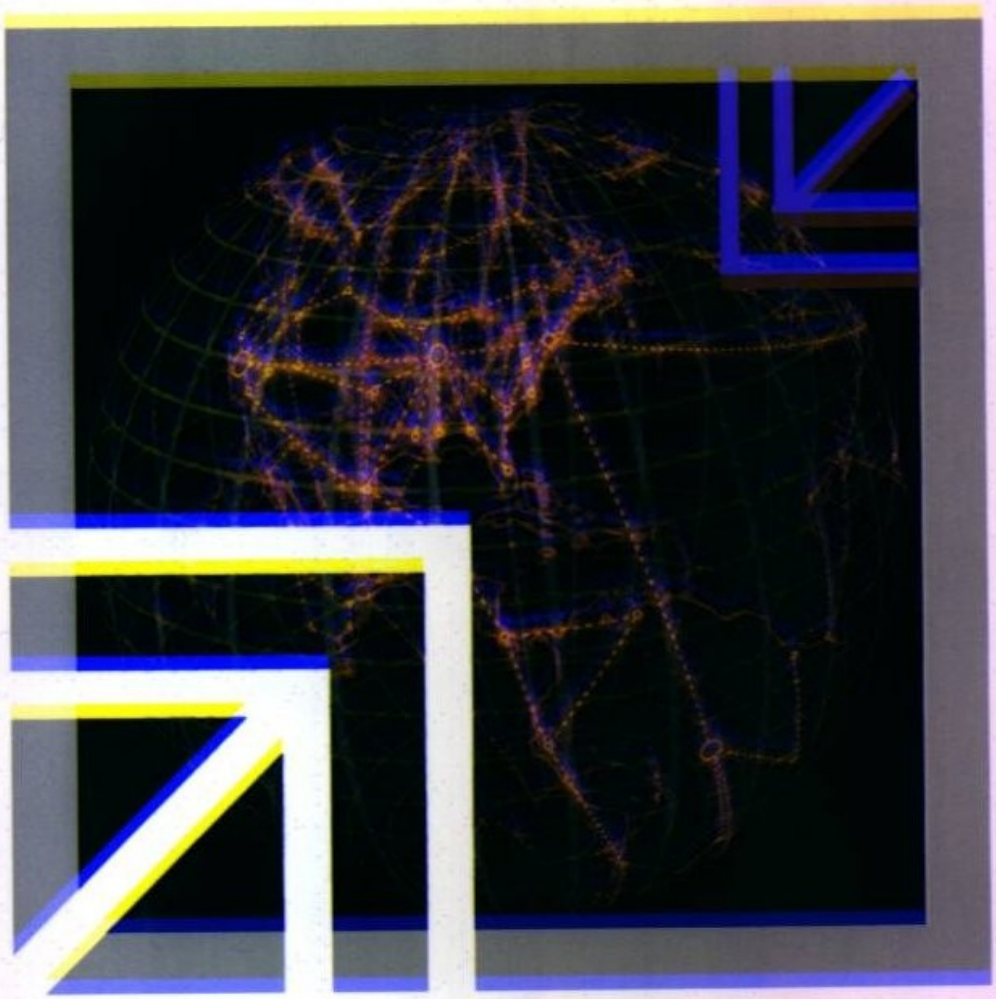

BEZPEČNOSŤ A BEZPEČNOSTNÁ VEDA

zborník vedeckých a odborných prác

2009

BEZPEČNOSŤ A BEZPEČNOSTNÁ VEDA

Zborník vedeckých a odborných prác

Zostavil:
doc. Ing. Ladislav HOFREITER, CSc.

Liptovský Mikuláš – Liptovský Ján
2009

Všetky články v zborníku boli recenzované.

Recenzenti :

brig. gen. doc. Ing. Miroslav KELEMEN, PhD., AOS L.Mikuláš
plk.gšt. doc. Ing. Pavel NEČAS, PhD., prorektor AOS L.Mikuláš
Dr.h.c.prof.Ing. Vladimír JANEČEK, DrSc., emeritný profesor AOS,
prof. Ing. Vojtech JURČÁK, PhD., KtB AOS L.Mikuláš
prof. dr. hab. Slawomir MAZUR, Akademia Krakowska, Krakow
prof.nadzw. dr.hab. Leszek KORZENIOWSKI, prezident EAS, Krakow
prof. nadzw., dr.hab. Jan MACIEJEWSKI, Wroclaw,
doc.V.M. ZAPALATINSKIJ, NAU Kijev, Ukrajina,
prof . Ing Vjačeslav BEREZUCKÝ CSc, CHPI, Charkov.
doc. Ing. Josef JANOŠEC, CSc., IOO Lázně Bohdaneč, ČR
doc. PhDr. František ŠKVRNDA, FMV EU Bratislava
doc. RSDr. Jozef MATIS, PhD., AOS L.Mikuláš
doc. Ing. Ladislav HOFREITER, CSc. AOS L.Mikuláš

Redakcia zborníka:
doc. Ing. Ladislav HOFREITER, CSc.

Články neprešli jazykovou úpravou.

ISBN : 978-80-8040-372-0

Predhovor

Bezpečnosť - slovo, spájané s pocitom istoty, je vyjadrením pocitu, že sa človek necíti byť ohrozený. Získať a udržať si tento pocit je v súčasnom svete čoraz ťažšie. Na človeka, sociálne skupiny, ale i národy a štáty doliehajú problémy, ktoré doposiaľ nemusel riešiť, alebo sa tieto nevyskytovali s takou intenzitou.

Po skončení Studenej vojny ľudstvo podľahlo eufórii, radosti z toho, že sa zabavilo strachu z globálnej vojny, z možnej apokalypsy sveta ako dôsledku riešenie nezmieriteľných , antagonistických konfliktov dvoch superblokov.

Ešte celkom nepominul strach z globálnej vojny, ako dominantného bezpečnostného problému, a už sa objavili nové bezpečnostné hrozby. Väčšina nových (?) bezpečnostných problémov nemá typický charakter vojenských ohrození, ale ich dôsledky sú často porovnateľné s dôsledkami vojen.

Bezpečnostná komunita musela v pomerne krátkej dobe prejsť od skúmania vojenských aspektov bezpečnosti k novým metódam a prístupom analýzy bezpečnosti. Je preto logické, že sa vedie spor o to, ktorý vedný odbor je vlastne kompetentný prioritne riešiť problémy bezpečnosti : **strategické štúdie, bezpečnostné štúdie, či sekuritológia ?**

Práve riešeniu tejto otázky je venovaná táto publikácia, ktorá vznikla ako výsledok diskusie medzinárodnej vedeckej bezpečnostnej komunity.

V jednotlivých príspevkoch sú prezentované názory na teoreticko-metodologické otázky bezpečnostnej vedy, terminológiu bezpečnosti, ale i na riešenie špecifických problémov v jednotlivých analytických sektoroch bezpečnosti či na problémy spojené s bezpečnostným vzdelávaním.

Vydanie zborníka je príspevkom k diskusii o potrebe bezpečnostnej vedy a bezpečnostného vzdelávania. Veríme, že čitateľ v ňom nájde odpovede na otázky, ktoré súvisia s týmito problémami.

Zborník bol vydaný ako súčasť riešenia projektu AgMO 9 : *Komplexná metodika hodnotenia bezpečnostného prostredia.*

doc. Ing. Ladislav HOFREITER, CSc.,
zostavovateľ zborníka

nemôže sa uzatvoriť do seba, ale musí sa cieľavedome „obklopovať" všeobecne akceptovateľnými vednými odbormi, ktoré sú uznávané vo vedeckej komunite. Najmä „civilná" – „nevojenská" a „nepolicajná" vedecká komunita vníma mnohé bezpečnostné témy, problémy, pojmy a kategórie z prostredia armády a polície s určitou nedôverou a pochybnosťami. To čo je vo vedecko-akademickej vojensko-policajnej komunite samozrejmé a všeobecne akceptovateľné, nemusí byť tak samozrejmé a jednoznačné aj pre širokú verejnosť. Z tohto dôvodu je dôležité formovať nielen vlastné metodologické „jadro" bezpečnostných a policajných vied, ale adekvátnym spôsobom rozvíjať aj celú sústavu, resp. systém rôznych pomocných a aplikovaných spoločenskovedných disciplín, ktoré tvoria vonkajší „sekuritologický" obal jadra bezpečnostnej vedy. Takúto úlohu môžu plniť práve rozvoj aplikovaných sociologických disciplín, medzi ktoré patrí aj policajná sociológia.

Literatúra:

BRUSTEN, M.: Polizeisoziologie und gesellschaftliche Praxis. Zu einem Diskussionspapier der Jungsozialisten über die „Polizei in der Klassengesellschaft", In: AJK (hrsg. v. M. Brusten/J. Feest/L. Lautmann), Die Polizei - eine Institution öffentlicher Gewalt, Luchterhand-Verlag, Neuwied/Berlin, 1974, S. 13-39.

HOFREITER, L.: Apológia bezpečnostnej vedy. In *www.defenceandtstrategy.eu, 15.6.2008*

LANGE, H.J.: *Innere Sicherheit im politischen System der Bundesrepublik Deutschland.* VS Verlag, 1999, s. 31, ISBN 3810022144.

LANGE, H.J.: *Die Polizei der Gesellschaft Zur Soziologie der Inneren Sicherheit,* 2003. s. 400-401, ISBN 978-3-8100-2879-2.

PÁNA, L. Sociologický „portrét" hospodářské elity v Ruské federaci. In *Medzinárodné vzťahy 2007, Aktuálne právne, kultúrne a sociálne otázky medzinárodných vzťahov,* Bratislava: Ekonóm 2008, s. 575-582, ISBN 978-80-225-2576-3.

REIMANN, H., B. GISEN, B., GOETZ, D., SCHMID, M.: *Basale soziologie: Teoretische Modelle,* VS Verlag, 1985, ISBN 3531114328, 9783531114323.

REUTER, M.: *Modernisierung der Landesverwaltung. Eine Implementationsstudie am Beispiel der Polizei in Nordrhein-Westfalen (NRW).* 2004, In: http://deposit.fernuni-hagen.de/249/1/Veroeffentlichung_1.pdf.

Vyhláška MŠ SR zo 7.5.1997 o doktorandskom štúdiu. Zbierka zákonov č. 131/1997, čiastka 61. In http://www.fei.stuba.sk/docs//2007/vyhl_131_97_PhD1.pdf

ЭКОНОМИКА СЕКЬЮРИТОЛОГИИ

Сергей ОХРИМЕНКО[1],

Совершенство достигается тогда, когда в исполнении не ошибаются и не медлят.
Ф.Ницше

Введение

Современное общество, вступив в фазу постиндустриального развития, получает все большую зависимость от информационных и коммуникационных технологий, которые превратились в доминирующий фактор развития личности, общества и государства. Вместе с тем, именно информационные и коммуникационные технологии (ИКТ) и их компоненты (сети, системы, программное обеспечение и т.д.), кроме положительных изменений в управлении социально-экономическими процессами, таят в себе новые опасности и риски. Следует отметить, что невнимание и недооценка существующих опасностей и угроз приводит к серьезным экономическим последствиям. Непонимание серьезности последствий совершенно не означает, что данной проблемы не существует. Скорее наоборот, спектр угроз и рисков постоянно возрастает, что приводит к пересмотру структуры и состава средств противодействия правонарушениям в среде сбора, обработки и распространения информационных продуктов и услуг.

Функционирование личности, общества и государства проходит в различных сферах, в рамках которых возможно воздействие неблагоприятных факторов и угроз. Интересна точка зрения известного русского философа Н.Бердяева, который рассматривал историю как арену коллективного творчества. В тоже время, история соткана из преступлений, для нее характерна катастрофичность [5]. Человек вступая в современный мир «страшится мирового механизма природы». Новая эпоха характеризует взаимодействие человека не с природой, а «реальностью машины, техники, которых в природе нет» [6].

«Моральное и духовное развитие человека не соответствует техническому развитию и … это создает главную причину нарушения равновесия человека» [6]. Человек отрывается от природы и погружается в замкнутый социальный мир. Автономная власть техники приводит к потере человеком духовного равновесия. Человек становится рабом собственных открытий. Как отмечается в [34], «…и сам человек, вместе с развитием цивилизации, порождает все новые и большие угрозы»

Возникновение на стыке веков новой междисциплинарной науки, какой является секьюритология, вызвало повышенный интерес со стороны специалистов, работающих в различных областях знаний. Существенную роль в становлении секьюритологии играет Европейская Ассоциация по Безопасности, которую возглавляет Л.Корженевски [34]. Благодаря этому, произошел существенный сдвиг в оценке методов и средств формирования внутренней и внешней безопасности. Безопасность, в широком смысле этого термина, стали рассматривать как совокупность экономической, социальной, политической, военной, экологической, технологической, культурной, интеллектуальной, информационной, демографической, психологической и многих других составляющих. По нашему мнению, в основе всех видов деятельности находится информационная составляющая. Без научно-технической информации невозможна производственная и экономическая деятельность, без сбора и обработки соответствующей информации не удастся сформировать, например, объективную

[1] д.э.н., профессор, Лаборатория информационной безопасности, Молдавская Экономическая Академия http://security.ase.md

экологическую картину государства или региона. Производство и распределение электроэнергии невозможно без использования информационных систем и т.д. Таким образом, все виды человеческой деятельности напрямую связаны с информацией, от объема сбора, обработки и достоверности которой, зависит качество принимаемых управленческих решений.

Становление экономики секьюритологии

За последнее время, все больше внимания уделяется экономическому анализу проблем информационной безопасности. Ключевой проблемой информационного общества становится появление все большего количества товаров и услуг, связанных с использованием информационно-коммуникационных технологий и программного обеспечения. Вместе с большим количеством новых продуктов пользователи сталкиваются с новыми угрозами, обусловленными недоработками в программном обеспечении (уязвимостями), разработкой вредоносных программ. Динамика роста вредоносных программ приведена в таб.1.

Таблица1

Динамика роста вредоносных программ

Год	2001	2002	2003	2004	2005	2006	2007	3 квартал 2008
Количество вредоносных программ	8821	11136	20731	31726	53950	169689	472621	1315474

Источник: данные «Лаборатории Касперского» за 2008 год

По данным Computer Economics в мире снижается общий ущерб от злонамеренных компьютерных атак. Если в 2004 г. он составлял 17,5 млрд. долл., то в 2006-м только 13,3 млрд. Этот результат, как считают эксперты, обусловлен появлением на рынке и массовым внедрением в пользовательской среде эффективных средств защиты [20]. По данным организации CSI, компании, участвующие в ее опросах, отметили двукратный рост убытков от атак: 345 тыс. долл. в среднем на компанию в 2007 г. против 166 тыс. в 2006-м. По сообщениям электронных средств массовой информации в 2008 году было осуществлено 190 тысяч атак и, их реализация принесла около 20 млн. долларов прибыли.

Экономика секьюритологии, как самостоятельное научное направление получило развитие в 90-х годах прошлого столетия. Истоками данного направления следует считать комплекс исследований и практических разработок, связанных с такими факторами, как:

- процессы совершенствования организационных форм использования вычислительной техники;
- заменой вычислительной базы и переходом к использованию новых информационных и коммуникационных технологий;
- разработкой операционных систем для персональных компьютеров;
- появлением специфических угроз (компьютерных вирусов);
- реализацией атак на информационные системы и другие.

Приведенные факторы во многом взаимосвязаны. Например, появление персональных компьютеров привело к персонализации вычислительных процессов, а это вызвало изменения в организационных формах использования не только вычислительной техники, но и организации технологических процессов сбора, регистрации, обработки и хранения информации. Рассмотрим подробнее приведенные факторы.

В начале 80-х годов оформилась новая отрасль – информационно-вычислительного обслуживания (ИВО). Это обусловило возможность использования единых подходов к управлению процессами преобразования информации, их организации и планирования. В то же время, специфика деятельности и технико-экономические особенности вызвали потребность в разработке комплекса вопросов, связанных с определением трудоемкости работ и услуг, составлением техпрофинплана и др. [4,8,10,18]. Получили также развитие работы, направленные на формирование планов производственно-хозяйственной деятельности вычислительных установок (пятилетних и годовых), экономического анализа деятельности вычислительных установок [22,24,25,29,32].

Проблема совершенствования организационных форм использования вычислительной техники не является новой в силу того обстоятельства, что она стала рассматриваться, начиная с момента использования первых ЭВМ в процессах управления производственными и экономическими объектами. При решении комплекса вопросов, связанных с повышением их эффективности, самостоятельное направление получили исследования, направленные на:

- совершенствование организационной структуры и производственно-хозяйственной деятельности;
- повышение эффективности процессов проектирования и эксплуатации информационных систем и сетей ЭВМ;
- разработкой специализированных инструментальных средств автоматизации программирования и сопровождения программных продуктов, промышленную эксплуатацию информационных ресурсов, баз и баз и банков данных на основе искусственного интеллекта и многие другие.

Развитие и совершенствование средств вычислительной техники выдвинули на первый план необходимость исследования проблемы эффективности их функционирования. Пионерскими работами в данном направлении следует признать труды С.П Куценко [8,17] и О.В.Голосова [11], в которых последовательно рассматривались вопросы становления индустрии информации, процессы проектирования, организации и планирования производственно-хозяйственной деятельности вычислительных центров.

Появление специализированной формы использования вычислительной техники – вычислительной установки, получило соответствующее отражение в научной и практической литературе [2,7,12-16,19,30]. Началась подготовка специалистов по курсу «Экономика и организация вычислительных установок».

Появление первых персональных компьютеров вызвало «информационный» бум, привело к пересмотру концепции построения вычислительных систем и сетей, автоматизированных систем управления предприятия (АСУП). Несмотря на развитие теории и практики внедрения АСУ, базирующихся на использовании ЭВМ третьего поколения, следует отметить ряд негативных черт, присущих этому этапу развития средств и программ автоматизированной обработки информации [2,23,30,31]. Во-первых, существующие системы обработки данных все еще оставались достаточно дорогостоящими, а их эксплуатация — весьма трудоемкой. По этой причине, как правило, они использовались только на крупных предприятиях, имевших парк необходимой вычислительной техники и отделы АСУП с квалифицированным

персоналом, способным обеспечить процесс разработки и эксплуатации этих систем. Во-вторых, у ЭВМ третьего поколения отсутствовали развитые диалоговые средства, что отчуждало конечного пользователя информации от процесса ее обработки. Это сказывалось на недостаточно высокой степени оперативности решения задач, поскольку этот процесс состоял из ряда технологических этапов автоматизированной и ручной обработки данных.

Угрозы безопасности

Требования к безопасности и механизмам превентивной защиты в сфере информационных технологий должны быть адекватны потенциальным угрозам со стороны нарушителя. Это означает, что при проектировании, разработке и внедрении механизмов безопасности необходимо принимать во внимание возможные типы атак на механизмы их реализации.

Возможные угрозы можно объединить в следующие группы [3,21,26-28,33 и др.]:

1. *Пассивное наблюдение* – является сегодня одной из самых распространенных угроз. Это обусловлено, во-первых, относительной простотой реализации, а во-вторых, сложностью обнаружения со стороны системы безопасности информационной системы (ИС).

2. *Воздействие на обменную информацию*. Выражается в том, что злоумышленник перехватывает информацию, видоизменяет ее и отсылает получателю. В итоге получатель уверен, что он аутентифицировался с законным участником протокола, а на самом деле – со злоумышленником. Последствия подобного типа атак могут быть катастрофическими для введенного в заблуждение участника, так как в первую очередь нарушается целостность передаваемой информации. Для приложений, где целостность является главным требованием системы безопасности, нарушение ее и передаваемых сообщений создает соответствующий риск в виде прямых потерь.

3. *Изменение структуры протокола*.. Суть данных атак состоит в том, что злоумышленник видоизменяет структуру протоколов, после чего законные участники в процессе аутентификации не могут закончить протокол. Последствия могут быть самыми разнообразными – от простого отказа в обслуживании, до получения нарушителем доступа к ресурсам информационной системы.

4. *Видоизменение механизмов принятия решений*. Данный класс атак не является прямой атакой, но используется достаточно часто. Он состоит в видоизменении механизмов принятия решений, и используется, когда готовится атака на конкретного участника информационного взаимодействия.

Рассмотрим наиболее распространенные угрозы (рис.1).

Криптоанализ. Криптоанализ является самым известным методом атаки на любые модели защиты, использующие криптографические операции. Но со становлением криптографии, как отдельной отрасли науки, информационная индустрия пришла к решениям, которые сводят к минимуму усилия криптоаналитика. На практике стратегия криптоаналитика заключается в анализе и разработке атаки на протокол и только в случае неудачи – в атаке криптоалгоритма, что, как правило, требует значительных вычислительных ресурсов и инвестиций. Сегодня большинство пользователей, использующих криптографию для защиты своей информации, выбирают стандартные криптоалгоритмы, прошедшие апробацию, что делает атаку методом криптоанализа на применяемые механизмы практически невозможной.

Перехват обменной информации. Перехват сообщений – это несанкционированное чтение информации. При применении криптографических методов защиты для

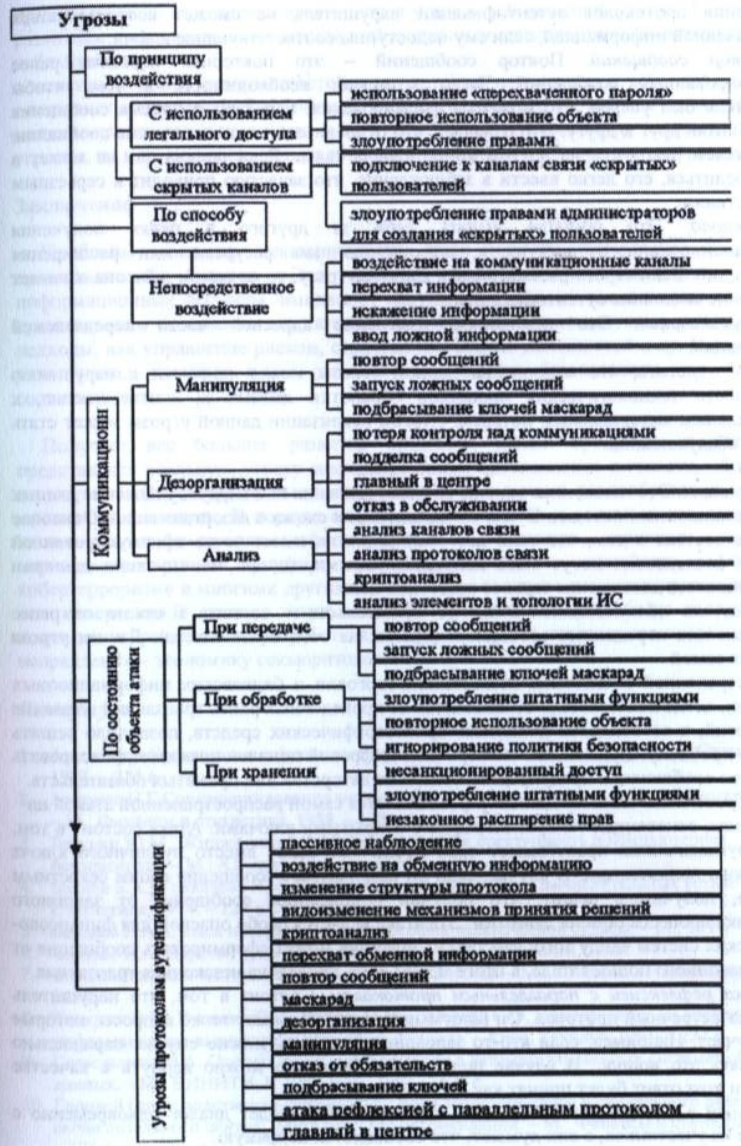

Рис. 1. Классификация угроз безопасности

построения протоколов аутентификации нарушитель не сможет воспользоваться перехваченной информацией, если ему недоступны соответствующие ключи.

Повтор сообщений. Повтор сообщений – это повторная передача ранее регистрированных сообщений. Часто возникает необходимость в том, чтобы получатель был уверен, что моменты формирования, передачи и приема сообщения очень близки друг к другу. Это означает, что отправитель в момент приема сообщения получателем находится на другом конце канала связи. Если получатель не может в этом убедиться, его легко ввести в заблуждение, что зачастую приводит к серьезным последствиям.

Маскарад. Это попытка выдать себя за другого в целях получения несанкционированного доступа к информационным ресурсам или расширения полномочий. Если строго рассматривать данную угрозу, то на самом деле она означает нарушение состояния аутентификации.

Дезорганизация. Это незаконное изменение адресной части передаваемой информации.

Следует отметить, что недооценка данной угрозы может привести к нарушению целостности технологических процессов обработки данных и, соответственно, к значительным материальным потерям. Итогом реализации данной угрозы может стать отказ в обслуживании.

Манипуляция. Это незаконная замена, вставка, удаление или переупорядочение данных в информационных потоках. В чем-то манипуляция схожа с дезорганизаций. Основное отличие состоит в том, что если дезорганизация не имеет четко сформулированной цели, и последствия могут быть непредсказуемыми, то при манипуляции данными предполагается достижение заранее известной цели.

Отказ от обязательств. Отказ от обязательств – состоит в отказе от ранее принятых или переданных сообщений (взятых на себя обязательств). Данная угроза является самой

распространенной в системах электронной торговли и банковских информационных системах, когда пользователь отказывается от проведенных ранее транзакций. Развитие технологий, в особенности появление криптографических средств, позволило решить данную проблему. Применение электронной цифровой подписи позволяет фиксировать авторство сообщения и предупредить отказы от авторства или принятых обязательств.

Подбрасывание ключей. Данная угроза является самой распространенной атакой на протоколы, основанные на криптографии с открытыми ключами. Атака состоит в том, что злоумышленник представляет свой публичный ключ вместо публичного ключа легального пользователя. В случае, если он подписывает сообщение своим секретным ключом, получатель решит, что получил подписанное сообщение от законного участника процесса обмена данными. Эта атака является особо опасной для финансово-банковских систем ввиду того, что злоумышленник может сформировать сообщение от имени законного пользователя, в итоге может быть проведена незаконная транзакция.

Атака рефлексией с параллельным протоколом. Состоит в том, что нарушитель начинает встречный протокол. Он (злоумышленник) посылает те же вопросы, которые он получает. Например, если кто-то запрашивает пароль, можно ему же параллельно адресовать это вопрос. В случае получения ответа, его можно вернуть в качестве ответа, и этот ответ будет принят как верный.

Главный в центре. Состоит в том, что нарушитель ведет диалог одновременно с каждым из участников, а они думают, что сообщаются напрямую.

Однозначное отнесение конкретной угрозы к той или иной группе затруднено ввиду их сложности и разносторонности. Но с уверенностью можно определить

принадлежность отдельных характеристик угроз к той или иной группе. Более того, с развитием информационных технологий и теории анализа протоколов аутентификации наблюдается

появление видов и разновидностей атак, которые совмещают в себе две или более описанных выше угроз. Это означает, что при разработке протоколов аутентификации должны приниматься во внимание их стойкость по отношению не только к обычным угрозам, но и их модификациям и объединению в более сложные, интегрированные.

Заключение

Проблемы экономики секьюритологии стали получать пристальное внимание у представителей бизнеса. Это можно объяснить необходимостью защиты информационных ресурсов, имиджа от нарушения безопасности, которые приводят к существенным экономическим потерям. В настоящее время получают развитие такие подходы, как управление риском, страхование, анализ уязвимостей и др. В тоже время роль лица, принимающего решения в области безопасности, не получила соответствующего отражения.

Получает все большее развитие «теневой» рынок продуктов и услуг, что представляет реальную угрозу информационной безопасности личности, общества и государства. Структура данного «теневого» рынка весьма разнообразна и включает множество сегментов. В первую очередь, это относится к деятельности, связанной с такими категориями, как «фишинг», «спам», «хакинг», «крэкинг», «кардинг», «присвоение системы», «спуфинг», «теневые вычисления», «инсайдер», «оффшорный кибертерроризм» и многими другими. Отмечается создание специализированных групп «по интересам».В связи с этим мы остро нуждаемся в разработке теоретических подходов и практических разработках, направленных на становление нового научного направления – экономику секьюритологии.

Литература

1. Азеев и др. Организация и функционирование вычислительного центра. –М.: Статистика, 1977. – 215 с.
2. Антонов Н.Г Совершенствование механизма функционирования вычислительных центров. – М.: Финансы и статистика, 1988. – 128 с.
3. Батурин Ю.М., Жиджишский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юридическая литература, 1991. – 162 с.
4. Баянов Б.Х., Толкачева Л.М. Планирование и учет работы вычислительных установок. – М.: Статистика, 1974. – 128 с.
5. Бердяев Н.А. Смысл истории. Опыт философии человеческой судьбы. – М.: 1990.
6. Бердяев Н.А. Царство духа и Царство Кесаря. –М.: Республика, 1995.
7. Вычислительные центры коллективного пользования. – М.: Финансы истатистика, 1982. – 271 с.
8. Галицын В.К., Куценко С.П., Куттер М.И., Лазарева С.Ф. Планирование на предприятиях информационно-вычислительного обслуживания. – Киев: Тэхника, 1991. – 221 с.
9. Герасименко В.А. Основы защиты информации в автоматизированных системах обработки данных. – М.: ВИНИТИ, N 1080-В-91, 1991. – 478 с.
10. Годовой (производственно-финансовый) план экономического и социального развития вычислительного центра: Методические рекомендации. – М.: Финансы и статистика, 1981. – 175 с.
11. Голосов О.В. Экономическое стимулирование системной обработки информации. – М.: Финансы и статистика, 1982. – 200 с.

12. Доветов М.Ш., Залесов В.А. Экономика и организация вычислительных установок. – М.: Финансы и статистика, 1982. – 303 с.
13. Исаков В.И., Кастерин В.И., Подольский В.И. Экономика, организация и планирование работы машиносчетных установок. – М.: Статистика, 1974. – 264 с.
14. Каныгин Ю.М. Экономика и организация машинной информатики. – Киев: Наукова думка, 1984. – 159 с.
15. Кустовые вычислительные установки. – М.: Статистика, 1978. – 231 с.
16. Кутер М.И. Эксплуатация ЭВМ в условиях хозяйственного расчета. – М.: Финансы и статистика, 1990. – 143 с.
17. Куценко С.П., Мариненко Б.В., Кривоносов Ю.Г. Экономика, организация и планирование вычислительных установок. – М.: Статистика, 1980. – 231 с.
18. Мелнгал А.Р. Организация оперативного планирования и составления техпрофинплана вычислительной установки. – М.: Статистика, 1978. – 151 с.
19. Новицкас Ю.М. Экономика ЭВМ. – Л.: Машиностроение, 1983. – 176 с.
20. Общий ущерб от злонамеренных компьютерных атак. http://www.itsec.ru/newstext.php?news_id=42731
21. Охрименко С.А., Черней Г.А. Угрозы безопасности автоматизированным информационным системам (программные злоупотребления). //Научно-техническая информация. Серия 1. Организация и методика информационной работы. – 1996, № 5, с.5-13.
22. Скоромнюк М.А. Эффективность организационных форм использования ЭВМ. – М.: Экономика, 1978. – 126 с.
23. Соколова Г.Н. Информационные технологии экономического анализа. — М.: «Экзамен», 2002 . — 320 с.
24. Соделль Б.Б. Эффективность ВЦ в условиях интенсификации информационно-вычислительного производства. – Рига: Зинатне, 1988. – 198 с.
25. Управление вычислительным центром./Под ред. Ю.П.Ларшина. – М.: Финансы и статистика, 1987. – 288 с.
26. Черней Г.А. Проблемы аутентификации в информационных системах. – Кишинев: Реклама, 2001. – 112 с.
27. 25. Черней Г.А., Охрименко С.А., Ляху Ф.С. Безопасность автоматизированных информационных систем. – Кишинев: Ruxanda, 1996. – 186 с.
28. 26. Черней Г.А., Охрименко С.А. Анализ на надеждността на протоколите за аутентификация. //Управленски, информационни и маркетингови аспекти на икономическото развитие на балкански страни. София: УНСС, 2004, с.263-277.
29. Чумаченко Н.Г., Заботина Р.Н. Анализ экономических результатов использования вычислительной техники: Методология и практика. – М.: Финансы и статистика, 1985. – 152 с.
30. Экономика индустрии информатики /Под ред. Ю.М. Каныгина, А.М.Меняйло. – Красноярск: Изд-во Краснояр. Ун-та, 1987. – 336 с.
31. Экономика и организация вычислительных установок./Под ред. В.И.Подольского. – М.: Финансы истатистика, 1987. – 271 с.
32. Якушенко В.Г. Планирование, учет и анализ деятельности хозрасчетных вычислительных установок. М.: Статистика, 1980. – 112 с.
33. Ярочкин В.И. Секьюритология – наука о безопасности жизнедеятельности. –М.: Ось, 2000.
34. Korzenowski L. Securitologia. Nauka o bezpieczenstwie czlowieka i organizacji spolecznych. – Krakow: EAS, 2008

ТЕОРЕТИЧЕСКИЕ ПРЕДПОСЫЛКИ РАЗВИТИЯ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ КАК НАУЧНОЙ ДИСЦИПЛИНЫ

Я.А.СЕРИКОВ[1]

РЕЗЮМЕ *Рассматриваются теоретические основы исследования с целью дальнейшего прогнозирования надежности функционирования антропогенных систем на основе технической диагностики. Предлагаемое направление включает теорию контролеспособности и теорию распознавания образов, которые в сочетании позволяют решать задачи обеспечения безопасности жизнедеятельности в подсистеме «человек - антропогенная система - окружающая среда».*

Одним из логических результатов эволюции человечества, его деятельности, является создание антропогенных систем разнличной структуры, сложности, назначения (технических, биологических, химических и др.). Такие системы предназначены для удовлетворения нужд человека разного иерархического уровня. Каждая из таких систем отличается качественными показателями и уровнем потенциального отрицательного воздействия на человека, производственную среду, биосферу Земли.

Степень безопасности систем обусловлавливается наличием и частотой отказов во время их функционирования, возможностью прогнозирования типа и времени реализации аварийных ситуаций. Таким образом, прогнозирование отказов, выявление причин их возникновения позволяет своевременно принять необходимые меры к их предупреждению и тем самым повысить безопасность, надежность и эффективность эксплуатации систем. Практика свидетельствует, что такой подход к эксплуатации системы позволяет получить экономический эффект около 30 % от ее эквивалентной стоимости [4, 5]. Рассматривая предупреждение влияния отказов системы на безопасность жизнедеятельности человека в комплексе, к указанному экономическому эффекту прибавляется существенное устранение отрицательного влияния последствий отказов системы на экологию Земли, например, через аварии, которые сопровождаются выбросом вредных веществ, опасных вирусов, микробов, появления электромагнитных и ионизирующих полей значительной напряженности и т. п. Положительный эффект достигается также за счет защиты здоровья населения как от возможных аномальных изменений физиологических функций, так и психологического состояния организма человека, обеспечения комфортности производственной, бытовой и среды проживания [2, 5].

[1] профессор, Харьковской национальной академии городского хозяйства член *EUROPEAN ASSOCIATION for SECURITY*,

4. Висновки

1. Виходячи зі встановленої потужності українських ТЕС, близько 36400 МВт, можна вважати, що сумарний річний викид українських ТЕС складає величину близько 21144031 тонн.
2. Якщо врахувати, що потужність ТЕЦ і опалювальних казаних зіставно з потужністю ТЕС, то орієнтування можна стверджувати, що сумарний викид українських теплогенеруючих об'єктів складає величину близько 42 мл. тонн.
3. При реалізації 3 % ризику в системах водоочистки ТЕС і ТЕЦ, додатково буде викинуто в повітряний басейн приблизно 1068085 т. шкідливих речовин.
4. При реалізації 3 % ризику в системах водоочищення призводить до скорочення тривалості життя людини приблизно на 1,5 місяця.

Література

1. БЕЛОКОНОВА А.Ф. Водно-химические режимы тепловых электростанций / Анна Федоровна Белоконова. – М.: Энергоатомиздат, 1985. – 201 с.
2. КОСТРИКИН Ю.М. Водоподготовка и водный режим энергообъектов низкого и среднего давления: Справочник / Кострикин Ю.М., Мещерский Н.А., Коровина О.В. – Энергоатомиздат, 1990. – 254 с.
3. Разработка комплексной безотходной технологии утилизации сточных вод ТЭЦ БКХЗ: Отчет о НИР / Северодонецкий технологический институт ВУГУ; № 83936937. – Северодонецк, 1993. – 200 с.
4. УРЯДНІКОВА І.В. Ресурсозберігаюча технологія підготовки теплоносія для теплових енергоустановок: Дис… канд. техн. наук: 05.14.14 / Уряднікова Інга Вікторівна. – Одеса., 2001. – 200 с.
5. ПРИСЯЖНЮК В.А. Анализ воды: цели, методы, прогнозирование свойств // Сантехніка, опалення, кондиціювання. – Київ, 2005. - № 5. – С.8-12.
6. СТОЛЬБЕРГ Ф.В. Екология города / Фелікс Владимирович Стольберг. – Киев: Либра, 2000. – 464 с.
7. ДЭВИНС Д. Энергия / Джон Дэвинс. – М.: Энергоатомиздат, 1985. – 360 с.

Názov :	**BEZPEČNOSŤ A BEZPEČNOSTNÁ VEDA. Zborník vedeckých a odborných prác.**
Editor :	Ladislav HOFREITER
Vydala :	Akadémia ozbrojených síl generála M. R. Štefánika so sídlom v Liptovskom Mikuláši
Náklad :	110 výtlačkov
Počet strán :	473
Vydanie :	prvé
Formát :	A 5
Tlač :	Tlačiareň Akadémie ozbrojených síl gen. M. R. Štefánika so sídlom v Liptovskom Mikuláši
Grafický návrh obálky:	Róbert Kandrik
Vydané :	2009

ISBN 978-80-8040-372-0