**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

ІНСТИТУТ КІБЕРНЕТИКИ ІМЕНІ В.М. ГЛУШКОВА НАН УКРАЇНИ

КІРОВОГРАДСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

**НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
ім. М.Є. ЖУКОВСЬКОГО «ХАІ»**

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

СОФІЙСЬКИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ, БОЛГАРІЯ

**ВІЙСЬКОВА АКАДЕМІЯ ЗБРОЙНИХ СИЛ
АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ**

**УНІВЕРСИТЕТ ТЕХНОЛОГІЇ І ГУМАНІТАРНИХ НАУК
(м. БЕЛЬСЬКО-БЯЛА, ПОЛЬЩА)**

**ПЕРША МІЖНАРОДНА
НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ**

ПРОБЛЕМИ НАУКОВО-ТЕХНІЧНОГО ТА ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У СУЧАСНОМУ СВІТІ «ПНПЗК-2016»

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

30 БЕРЕЗНЯ – 1 КВІТНЯ 2016 РОКУ

**ХАРКІВ – КИЇВ – КІРОВОГРАД – ВІННИЦЯ –
СОФІЯ – БАКУ – БЕЛЬСЬКО-БЯЛА
2016**

УДК 621.387 : 681.327 ПРОБЛЕМИ НАУКОВО-ТЕХНІЧНОГО ТА ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У СУЧАСНОМУ СВІТІ: Матеріали першої міжнародної науково-практичної конференції. – Харків, НТУ «ХПІ»; Інститут кібернетики ім. В.М. Глушкова НАН Україні, Київ;КНТУ, Кіровоград; ВНТУ, Вінниця; НАУ ім. М.Є. Жуковського «ХАІ»; ХНУРЄ, Харків; Софійський технічний університет, Болгарія; Військова академія збройних сил Азербайджанської республіки; Університет технології і гуманітарних наук, Бельсько-Бяла, Польща., 2016. – 60 с.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

ПЛЕНАРНЕ ЗАСІДАННЯ

РОЛЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ МЕЖДУНАРОДНЫХ КОМПАНИЙ В ЭКОНОМИКЕ УКРАИНЫ.

д.т.н., проф. Алішов Н.І.-о., Інститут кібернетики ім. В.М. Глушкова НАН України, Київ; Алишов Г.Н., Национальная академия управления, Киев

Технология вложения инвестиций международных компаний в Украину для взаимного развития экономических отношений представляется актуальной научно-экономической задачей. Однако существует вероятность использования объективных уязвимых экономических трудностей в Украине для использования этих уязвимостей в пользу инвестирующих компаний. Наличие всех законодательных положений, регулирующих эти взаимоотношения не всегда способны противостоят этому процессу по ряду причин. Поэтому существующая организационная инфраструктура контроля финансовой инвестиционной деятельности в принципе не способны объективно регулировать экономические взаимоотношения между Украиной и этими компаниями. Международный опыт показывает, что для решения этой проблемы необходимо внедрять современные информационные технологии между экономически взаимодействующими субъектами. Исходя из этого, предлагается внедрения следующей схемы взаимодействия между инвестиционными компаниями и государством. Создается хранилище данных (*DATAWAREHOUSE*), где для каждой компании выделяются отдельные витрины данных. Эти данные обрабатываются технологией многомерной оперативной аналитической обработкой (*OLAP* технология). Далее эти данные передаются подсистеме интеллектуального выявления хронологических закономерностей (*DATA MINING*), которая выдает шаблоны знаний о деятельности этих компаний для системы поддержки приятия решений. Кстати при этом возможно выявить уязвимости в деятельности, в том числе в государственном управлении. При этом государство должно гарантировать неразглашения финансовой деятельности международных компаний. Для этого необходимо организовать предельно высокую безопасность внедряемых информационных технологий. На сегодняшний день существуют множество вариантов решения кибербезопасности таких возможностей: использования виртуальных частных сетей, внедрения интеллектуальных логико-контетных систем фильтрации типа *ISA SERVER* и т.п. В докладе будут подробно изложены особенности предлагаемых решений.

ОСНОВНІ ВЛАСТИВОСТІ НОВОГО НАЦІОНАЛЬНОГО СТАНДАРТУ БЛОКОВОГО ШИФРУВАННЯ ДСТУ 7624:2014

д.т.н., доц. Олійников Р.В., ХНУ ім. В.Н. Каразіна, Харків; д.т.н., проф. Горбенко І.Д., ПАТ "Інститут інформаційних технологій", Харків

У доповіді розглянуті принципи побудови і основні властивості нового національного стандарту криптографічного перетворення ДСТУ 7624:2014, що визначає блоковий шифр "Калина" та режими його роботи. Шифр побудований на основі Rijndael-подібної структури та містить попереднє і прикінцеве забілювання (pre- and postwhitening) із використанням модульного додавання (2^{64}), чотири різні S-блоки, МДВ-перетворення зі збільшеним розміром матриці та нову односпрямовану схему розгортання циклових ключів. "Калина" підтримує різні комбінації розміру блоку і довжини ключа (128, 256 і 512 бітів). Криптографічне перетворення є стійким при 6 циклах для 128-бітового блоку, 7 циклах для 256-бітового та 9 циклах для 512-бітового. На 64-бітовій платформі швидкодія "Калини" вища або порівняна з AES, проте "Калина" забезпечує суттєво більш високий запас стійкості до криптоаналітичних атак. При відповідній довжині ключа швидкість "Калини" приблизно у 2 рази вища, ніж у нових стандартів шифрування Білорусії і Росії.

ПЛАНИРОВАНИЕ МНОГОФАКТОРНОГО ЭКСПЕРИМЕНТА ПРИ РАЦИОНАЛЬНОЙ ОРГАНИЗАЦИИ ТЕСТИРОВАНИЯ СИСТЕМ

д.т.н., проф. Раскин Л.Г., д.т.н., проф. Серая О.В., НТУ "ХПИ", Харьков

Решена задача отыскания гамильтонова пути на полнодоступном графе полного факторного эксперимента. Рассмотрен вариант постановки задачи, когда качество маршрута определяется только числом изменений уровня факторов. Анализируется возможность решения этой задачи методом ветвей и границ. Показано, что этот метод не может быть использован для решения задачи, в которой число факторов превышает четыре. Предложен простой неперебoрный метод точного решения сформулированной задачи. Рассмотрены другие, более сложные варианты этой задачи, приводящие к двухкритериальной схеме. При этом для решения задачи предложен Парето-подход. Приводятся примеры.

НЕЙРОННЫЕ СЕТИ КАК СРЕДСТВО РАСПОЗНАВАНИЯ АТАК НА КОМПЬЮТЕРНЫЕ СИСТЕМЫ

д.т.н., проф. Дмитриенко В.Д., к.т.н., доц. Заковоротный А.Ю., НТУ "ХПИ", Харьков

Анализ научно-технической информации по применению нейронных сетей (НС) в системах распознавания вредоносных воздействий (атак, вирусов)

на компьютерные системы показал, что НС получили определенное распространение в подобных системах распознавания. В частности, многослойные персептроны, которые использовались как в системах распознавания атак и антивирусных системах, так и в системах распознавания уязвимостей. Однако многослойные персептроны обладают рядом существенных недостатков: сложностью обучения, невозможностью самостоятельного дообучения в процессе эксплуатации системы, недостаточной изученностью вопросов обобщения обучающей входной информации, высоким уровнем ложных тревог. В связи с этим в докладе для разработки систем распознавания вредоносных воздействий предлагается использовать новые НС адаптивной резонансной теории и нейроассоциативной памяти. Приводятся архитектуры и алгоритмы функционирования этих НС. Показываются их преимущества перед персептронами.

СЕКЦІЯ 1
ПРОБЛЕМИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ТА ПРОГНОЗУВАННЯ ЗАГРОЗ КІБЕРБЕЗПЕКИ

Керівники секції: д.т.н., проф. Дмитрієнко В.Д., НТУ «ХПІ», Харків

Секретар секції: к.т.н., доц. Хавіна І.П., НТУ «ХПІ», Харків

1. МЕТОД РОЗРАХУНКУ ЙМОВІРНОСТІ КОМПРОМЕТАЦІЇ ПОВІДОМЛЕНЬ, ЯКІ ПЕРЕДАЮТЬСЯ ЗА МНОЖИНОЮ МАРШРУТІВ, ЩО ПЕРЕТИНАЮТЬСЯ, З ПОСЛІДОВНО-ПАРАЛЕЛЬНОЮ І КОМБІНОВАНОЮ СТРУКТУРОЮ

д.т.н., проф. Лемешко О.В., к.т.н., с.н.с. Єременко О.С., ХНУРЕ, Харків

У доповіді розглянуто метод розрахунку ймовірності компрометації повідомлення, яке передається за множиною маршрутів, що перетинаються за каналами і вузлами, з послідовно-паралельною і комбінованою структурою. Як показав проведений аналіз, аналітичний розрахунок ймовірності компрометації повідомлення є важливим етапом у ході розв’язання задач безпечної маршрутизації. Однак існуючі методи розрахунку ймовірності компрометації повідомлення запропоновані лише для випадку шляхів, що не перетинаються. При цьому використання шляхів, що не перетинаються, призводить до неефективного використання мережних ресурсів і зниження якості обслуговування за показниками продуктивності. На ряді числових прикладів проведений аналіз впливу на ймовірність компрометації повідомлення параметрів безпеки окремих елементів (каналів зв'язку) і фрагментів мережі. Показано, що запропонований метод дає більш точні результати розрахунку від 20% до 40% у більшості вхідних даних, ніж раніше відомий метод при його застосуванні до випадку використання шляхів, що перетинаються.

2. МЕТОДЫ КАЧЕСТВЕННОГО АНАЛИЗА РИСКОВ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

д.т.н., проф. Смирнов А.А., к.т.н., доц. Коваленко А.В., КНТУ, Кировоград

В данной работе разработан комплекс методов качественного анализа рисков разработки программного обеспечения, что позволило решить противоречие, возникающих при разработке ПО, и заключающееся в пренебрежении фирмами-разработчиками ПО факторов уязвимости безопасности ПО. В качестве решения указанной проблемы предложено использование разработанных методов качественного анализа и количественной оценки рисков разработки программного обеспечения. Разработан метод качественного анализа

рисков разработки программного обеспечения. Его отличительной особенностью является учет факторов эксплуатационных рисков, особенно риска невыявления уязвимостей ПО и оценка произвольного непротиворечивого конечного набора «квантов информации». Разработан метод количественной оценки рисков разработки ПО. Его отличительной особенностью является комплексное использование методики «Анализа дерева отказов» и способа оценки показателя чистой приведенной стоимости проекта разработки ПО с учетом негативных факторов возможного невыявления уязвимостей безопасности ПО.

3. ПРИМЕНЕНИЕ MAC ДЛЯ ЗАЩИТЫ КОМПЬЮТЕРНОЙ СИСТЕМЫ

к.т.н., доц. Хавина И.П., НТУ "ХПИ", Харьков

В докладе на основе анализа графа атак показано применение агентов, использующих временную логику для оценки вероятностных различий реального мира и его представлений этого же мира. Т.е. в дополнение к анализу набора миров, которые агент считает возможным, он выражает эти убеждения в терминах вероятности во времени. Модели атаки, представленные в виде графа атаки, обычно используются несколько раз, что и образует набор временных миров. Это позволяет противнику учиться на собственном опыте, определяя какие из путей получили высокую вероятность успешного взлома системы. Защитники, в свою очередь смогут получить знания о графе атак через повторные наблюдения определенных шаблонов (миров). Когда система находится под атакой, защитник будет иметь представления об выбранных путях атаки и об убеждениях противника в отношении успеха соответствующего пути. Таким образом, защитник может выбрать контрмеры эффективно воздействуя только по путям, где эти вероятности высокие и действительно представляют угрозу.

4. НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИНФОРМАЦИОННЫХ СИСТЕМ КАК СРЕДСТВО ПОВЫШЕНИЯ КИБЕРБЕЗОПАСНОСТИ

д.т.н., проф. Кривуля Г.Ф., к.т.н., с.н.с. Липчанский А.И., ХНУРЭ, Харьков.

От уровня защищенности современных информационных систем зависит национальная безопасность государства, имеющего развитую промышленную структуру в виде большого количества сложных информационных киберобъектов. Одной из основных тенденций развития современных методов обеспечения защищенности киберсистем является повышение достоверности и точности методов обнаружения вторжений и аномалий при нарушении правильного функционировании объекта. Данная задача решается непре-

рывным мониторингом состояния системы с использованием методов функционального диагностирования. При этом важной проблемой является прогнозирование и выявление начальной стадии возникновения вторжения или аномалии.

Для решения данной задачи предлагаются гибридные интеллектуальные технологии с использованием нейронечетких экспертных методов, которые позволяют прогнозировать возможность наступления аномалий и сбоев как отдельных элементов, так и объекта в целом.

5. ЧИСЛОВО-АНАЛІТИЧНА КОНЦЕПЦІЯ ВІЗУАЛІЗАЦІЇ РОЗВ'ЯЗКІВ ПРИКЛАДНИХ ЗАДАЧ

д.т.н., проф. Алішов Н.І.-о., Інститут кібернетики ім. В.М. Глушкова НАН України, Київ; д.т.н., проф. Швачич Г.Г., Ткач М.О., Національна металургійна академія України, Дніпропетровськ

Доповідь присвячено розподіленому моделюванню візуалізації векторів розв'язків прикладних задач на основі схем підвищеного порядку точності. Більш високе прискорення обчислень порівняно з кінцево-різницевим підходом ілюструється використанням аналітичних розв'язків, які дозволяють проводити обчислення одночасно та паралельно за всіма часовими шарами. Показано, що найбільш перспективним підходом до математичного моделювання прикладних задач слід вважати той, що ґрунтується на числово-аналітичних розв'язках.

Для проведення обчислювальних експериментів на базі застосування багатопроцесорної обчислювальної системи розроблено пакет прикладних програм (ППП), що реалізує розв'язок коефіцієнтних обернених задач теплопровідності методом математичного моделювання. ППП розроблено з урахуванням вимог об'єктно-орієнтованого програмування. ППП включає блок візуалізації даних, який дозволяє отримати будь-які необхідні дані для побудови гладких графіків або ізоліній на відповідних сітках.

6. СПОСІБ ПРОГНОЗУВАННЯ ПОШИРЕННЯ КОНТЕНТУ І ЗАПИТІВ НА НЬОГО У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ

д.т.н., с.н.с. Грищук Р.В., ЖВІ ім. С.П. Корольова, Житомир; к.т.н., доц. Молодецька К.В., ЖНАУ, Житомир

В доповіді розглянуто методологічний інструментарій для прогнозування динаміки поширення контенту і запитів на нього за даними контент-аналізу повідомлень у соціальних інтернет-сервісах (СІС). Встановлено, що контент-аналіз є перспективним інструментом виявлення деструктивних інформаційних посилів у СІС, й особливо таких, які характеризуються сугестичними властивостями латентного характеру. В основу розробленого мето-

ду покладено метрику самоподібності – показник Херста, який забезпечує виявлення постійної складової контент-функції і встановлення її природи. Перевагами даного способу прогнозування поширення контенту і запитів на нього у СІС є: виявлення постійної складової в досліджуваних процесах взаємодії акторів віртуальних спільнот, у разі виявлення ознак персистентності спосіб дозволяє встановити ознаки тренду ряду і створює передумови для організації системою забезпечення інформаційної безпеки держави ефективної інформаційної протидії на основі концепції синергетичного управління. Впровадження способу прогнозування сприяє ефективному розподілу витрат ресурсів на функціонування системи забезпечення інформаційної безпеки держави.

7. АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ ВЫЯВЛЕНИЯ КИБЕРАТАК НА РЕСУРСЫ КОММУНИКАЦИОННЫХ СИСТЕМ

д.т.н., с.н.с. Грищук Р.В., ЖВИ им. С.П. Королева, г. Житомир; к.т.н., с.н.с. Евсеев С.П., к.т.н., доц. Король О.Г., ХНЭУ им. С. Кузнеца, Харьков

В докладе рассмотрены результаты анализа основных групп методов, используемых для выявления кибератак с учетом современных тенденций их развития. Обосновывается необходимость применения метода оценивания информативности параметров потока входных данных для современных систем выявления атак с целью получения в дальнейшем, на его основе, количественных характеристик анализируемых данных. Впервые раскрыта сущность принципа комплексирования количественного и качественного подходов к построению современных методов выявления кибератак для организации эффективных систем обеспечения информационной безопасности коммуникационных систем.

8. КІБЕРІНЦИДЕНТИ: ПЕРЕДУМОВИ СКОЄННЯ ТА НАСЛІДКИ

д.т.н., с.н.с. Грищук Р.В. ЖВІ ім. С.П. Корольова, Житомир

Ретроспективний аналіз кіберінцидентів, що мали місце в останні роки у світі в цілому та в Україні зокрема й аналіз яких подано доповіді, дозволив зробити ряд важливих висновків. Кількість кіберінцидентів у світі невпинно зростає. Місце їх проведення не обмежується територіальними кордонами держав. Передумовами для виникнення кіберінциденту може бути довільний соціально- значущий привід – від утисків прав та свобод громадян у будь-якій державі – до питань нав'язування власної «демократичної» політики та «економічної свободи» державами лідерами державам, що розвиваються. Цілями кіберінцидентів переважно стають суб'єкти та об'єкти, вразливі до кібернетичних впливів. Наслідки від скоєння кіберінцидентів поширюються на усі без виключення держави світу – від країн з розвиненою економікою –

до країн, що розвиваються. Також показано, що аналіз проявів кіберінцидентів дозволяє виявити ті точки прикладання основних зусиль, кібернетичний вплив на які може призвести до колапсу процесів управління, які протікають в системі державного управління, системах життєзабезпечення, суспільстві тощо.

9. СИСТЕМНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ БАГАТОПРОЦЕСОРНОЇ СИСТЕМИ З РОЗПОДІЛЕНОЮ ОБЛАСТЮ ОБЧИСЛЕНЬ

д.т.н., проф. Алішов Н.І.-о., Інститут кібернетики ім. В.М. Глушкова НАН України, Київ; д.т.н., проф. Швачич Г.Г., Ткач М.О., Волнянський В.В., Національна металургійна академія України, Дніпропетровськ

Доповідь присвячено висвітленню процесів налаштування системного програмного забезпечення багатопроцесорної системи з розподіленою областю обчислень. Блоки системи комплектуються за допомогою засобів обчислювальної техніки масового виробництва. Багатопроцесорна система містить один майстер-вузол і *N* обчислювальних *slave*-вузлів, два керовані комутатори (*SW*1, *IB*1), реконфігуровану мережу для обміну даними між обчислювальними вузлами, систему збереження результатів обчислень, механізм резервування ключових компонентів, а також передбачає завантаження вузлів у мережі *GI* (*Gigabit Ethernet)* за допомогою комутатора *SW*1. Комунікаційна мережа системи орієнтована на використання технології *InfiniBand*. Режими керування багатопроцесорною системою здійснюється набором процесів, які виконуються в різних лезах і взаємодіють між собою. При цьому керування та передача відповідних даних із *slave*-вузлів відбувається за допомогою мережевих адаптерів. *З*берігання даних обчислень з метою їх подальшої обробки виконується за допомогою відповідної системи.

10. АЛГОРИТМ НАПРАВЛЕНОГО ПЕРЕБОРУ ДЛЯ МІНІМІЗАЦІЇ БУЛЕВИХ ФУНКЦІЙ

к.т.н., доц. Миронець І.В., ЧДТУ, м. Черкаси

З розвитком комп'ютерних технологій об'єм інформації все більше зростає, тому виникає необхідність вибору мінімальної та оптимальної інформації з усього потоку, вибору даних та створення запитів в базах даних, проектування та синтез комбінаційних схем. Булеві функції традиційно використовуються в якості математичних моделей цифрових пристроїв. Процедура мінімізації булевих функцій, як правило, застосовується на етапі логічного синтезу для отримання економічного представлення пристрою, що проектується. Задача для мінімізації функцій на більше ніж десять змінних на сьогоднішній день не вирішена, оскільки, всі існуючі методи стикаються з проблемою мі-

німізації функцій при збільшенні кількості змінних. Основною перевагою розробленого алгоритму є можливість його реалізації засобами обчислювальної техніки, а покладений в основу направлений перебір дозволяє зменшити вимоги до програмно-апаратних засобів автоматизованих систем проектування дискретних пристроїв.

11. МЕТОДЫ ИЗВЛЕЧЕНИЯ ОНТОЛОГИЧЕСКОЙ ИНФОРМАЦИИ В ПРЕДМЕТНОЙ ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

д.т.н., проф. Порошин С.М., Можаев А.А., Можаев М.А., НТУ "ХПИ", Харьков

Доклад посвящен методам извлечения онтологической информации из текстов естественного языка. Приведена теоретико-модельная формализация таких отношений между понятиями синонимия, "общее-частное", "одно понятие используется для определения другого понятия". Разработаны методы извлечения этих отношений, а также определений понятий из текстов естественного языка. Для анализа текстов использован язык описания лингвистических шаблонов.

Разработанная программная система показала достаточно высокую точность и полноту извлекаемых знаний. Она применяется при разработках экспертной системы по информационной безопасности и системы управления рисками при обеспечении информационной безопасности.

12. ПІДВИЩЕННЯ ШВИДКОДІЇ АРИФМЕТИЧНИХ ПРИСТРОЇВ НА ОСНОВІ ПОЗИЦІЙНОЇ СИСТЕМИ ЧИСЛЕННЯ

к.т.н., доц. Куницька С.Ю., ЧДТУ, Черкаси

В доповіді розглянуто дослідження моделі двійково-трійкової системи числення з оптимальною інформаційною надлишковістю, яка забезпечує підвищення швидкодії при зменшенні складності апаратної реалізації завдяки моделюванню арифметичних пристроїв. Синтезована система числення, вагові коефіцієнти розрядів якої задані послідовністю: 1, 2, 2, 6, 6, 18, 18, 54, 54, 162, 162, 486 є надлишковою і відповідно, введена інформаційна надлишковість можлива при використанні для знаходження помилок. Отримано логічний вираз математичної моделі пристрою контролю помилок.

Для оцінки швидкодії суматора проведено його моделювання, як суматора з груповим переносом, що формує кожна пара розрядів. Один з варіантів суматора для двійково-трійкової системи числення було представлено у вигляді дискретної моделі.

Доведено, що синтезований суматор для двійково-трійкової системи числення має складність на 16,6% менше складності реалізації без надлишкового суматора при однаковій швидкодії.

13. АНАЛИЗ МОДЕЛЕЙ ПОВЕДЕНИЯ ТРАФИКА

Шипова Т.Н., Гейко Г.В., НТУ "ХПИ", Харьков

Современные методы обнаружения вторжений в компьютерные сети не всегда способны выявить аномалии вызванные действием модификаций или новых видов атак. Это связано с тем, что в пространстве компьютерных сетей и систем насчитывается огромное количество видов атак, которое невозможно достаточным образом стандартизировать.

В последнее время для выявления аномалий в компьютерных сетях всё больше используются свойства фрактального самоподобия трафика, и поскольку инвариантная к масштабу пульсирующая структура трафика может оказывать сильное влияние на производительность сети, то анализ причин и последствий самоподобности в трафике является очень важной задачей. Причём инвариантная к масштабу пульсирующая структура является не отдельным, побочным явлением, а скорее характерной особенностью, сложившейся в пределах сетевых окружений.

Центральными понятиями фрактального анализа являются фрактальная размерность и показатель Херста. При помощи этих показателей можно сравнить характеристики трафика в интервале заданной размерности и, формализуя результаты сравнения можно делать вывод о наличии или отсутствии аномалии в определённый период времени.

Цель работы заключается в выборе оптимального параметра для создания моделей поведения трафика, что позволит сделать заключение о наличии или отсутствии самоподобия и сделает возможным обнаружить аномалии в сети.

14. РАСШИРЕНИЕ ОБЛАСТИ УСТОЙЧИВОСТИ ПРИ ПАРАЛЛЕЛЬНОМ МОДЕЛИРОВАНИИ

д.т.н., проф. Дмитриева О.А., ГВУЗ «ДНТУ», Красноармейск

Материал данного доклада ориентирован на разработку и обоснование методов моделирования динамических систем с расширенной областью устойчивости, обладающих высокими показателями параллелизма. В качестве исходного выбран класс методов с одной опережающей точкой типа Биккарта и осуществлена попытка увеличить количество расчетных точек, формирующих блок. Использование выражений для невязок и разложений в ряд Тейлора позволило сформировать общий вид системы алгебраических уравнений, обеспечивающей определение расчетных коэффициентов для любого количества опережающих точек. Для некоторых размерностей блоков приведены сгенерированные разностные расчетные схемы, ориентированные на количество доступных процессоров в параллельной реализации. Доказана абсолютная устойчивость по начальным данным и по правой части. На из-

вестных тестовых задачах с произвольной размерностью выполнена параллельная реализация разработанных методов.

15. МОДЕЛЮВАННЯ СТРАТЕГІЇ ЗАХИСНИКА З ВИКОРИСТАННЯМ БІОНІЧНИХ МЕТОДІВ ОПТИМІЗАЦІЇ

д.т.н., проф. Дмитрієва О.А., Бєлов Є.Г., ДВНЗ «ДНТУ», Красноармійськ

Роботу присвячено проблемам математичного моделювання функціонування скінченного автомата на прикладі гри «Війна за ресурси». Обрані для дослідження клітинні автомати дозволяють описувати системи, що характеризуються відносно простою структурою і, в той же час, складною поведінкою. Крім того, клітинні автомати тісно пов'язані з поняттям мультиагентних систем, будучи їх різновидом. Досліджено вплив вхідних параметрів алгоритмів на якість розв’язання, виявлено можливості модифікації алгоритмів, які можуть привести до покращення якості та скорочення часу моделювання, проведено порівняльний аналіз розроблених модифікацій з класичними алгоритмами. Розроблена модель гри «Війна за ресурси» відображає процес між нападаючим, діючим за стохастичною стратегією, і захисником, дії якого керуються скінченним автоматом. На основі отриманих експериментальних даних можна стверджувати про підвищення частки перемог захисника приблизно до 74%, якщо керування здійснюється за допомогою генетичних алгоритмів, та до 67% за допомогою алгоритму імітації відпалу.

16. ПІДВИЩЕННЯ ЯКОСТІ СТЕГАНОАНАЛІЗУ ЗА РАХУНОК ПОПЕРЕДНЬОЇ СЕГМЕНТАЦІЇ ЗОБРАЖЕНЬ

д.т.н., проф. Кучук Г.А., д.т.н, проф. Рубан І.В., Худов В.Г., ХУПС ім. І. Кожедуба, Харків

В роботі розглядається використання зображення у якості стеганографічного контейнеру. З цією метою проводиться попередня підготовка зображення для використання у якості контейнеру. При цьому повинні бути виключені з розгляду ті частини зображення, де характеристики заповненого та природного контейнеру потенційно не розрізняються.

Для вирішення указаної задачі запропоновано у якості попереднього етапу статистичного стеганоаналізу проводити сегментацію зображення. Сегментація зображення проводиться з метою визначення областей зображення, де значення яскравості пікселів неможливо передбачити (шум, контури, значні перепади яскравості та інші).

В роботі проводиться короткий огляд відомих методів статистичного стеганоаналізу, висвітлюються теоретичні методи сегментації зображення. Для виявлення ізольованих пікселей та виявлення шуму на зображенні запропоно-

вано використання лапласіану-гауссіану, лапласіану Канні, операторів Превітта, Собела та методу швидкого розрахунку модуля градієнта, коли за основу вибирається вертикально-горизонтальний градієнт, який потім коректується з урахуванням впливу діагональних сусідніх пікселів. Проводиться аналіз ефективності використання відомих методів сегментації зображення з метою проведення статистичного стеганоаналізу.

17. ИССЛЕДОВАНИЕ СПОСОБА КОНТРОЛЯ ЛИНИЙ СВЯЗИ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ ДЛЯ ОБЛАЧНЫХ АНТИВИРУСОВ

д.т.н., проф. Смирнов А.А., Смирнов С.А., к.т.н., доц. Дидык А.К., КНТУ, Кировоград

Проведенные исследования показали, что аппаратура, расположенная на стороне программного сервера контроля и анализа метаданных в облачных антивирусных системах, кроме основных своих функций должна включать в себя систему контроля и обнаружения несанкционированного доступа. В задачу этой системы должны входить: наблюдение за состоянием ВОЛС, контроль принимаемого сигнала и передача его в интеллектуальный ассоциативный блок нейросетевых решений, в котором и принимается решение о наличии несанкционированного доступа к ВОЛС.

Использование данного способа позволит выявлять изменение характеристик ВОЛС в процессе функционирования ТКС, (получить необходимые данные для начала процедуры обучения нейронных экспертов) и выдавать необходимые сигналы аномалий (возможных кибератак) в линиях связи в систему нейросетевых экспертов безопасной маршрутизации. Это позволит снизить вероятность манипуляций метаданными, передаваемыми в узлы программного сервера.

18. ВЫЯВЛЕНИЕ АНОМАЛЬНОГО ПОВЕДЕНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ С ПОМОЩЬЮ КОНТРОЛЬНЫХ КАРТ ШУХАРТА И КАРТ КУМЛЯТИВНЫХ СУММ

к.т.н., проф. Гавриленко С.Ю, д.т.н., с.н.с. Семенов С.Г., Горносталь А.А., НТУ "ХПИ", Харьков

Повсеметсное распространение компьютерных систем (КС) во всех сферах человеческой жизни влечёт за собой потребность в более жесткосм контроле качества их работы. Особая роль в этом вопросе отдаётся аналитическим алгоритмам, которые в режиме раельного времени способны выявить нарушения в работе той или иной вычислительной машины. В работе предстален сравнительный анализ применения контрольных карт Шухарта и карт кумулятивной суммы для выявления аномального поведенеия компьютерных

систем. Для получения данных и выполнения экспериментов была разработана компьютерная программа, с помощью которой были получены результаты для нескольких рабочих режимов. При этом были сделаны выводы, которые позволяют по результатам анализа состояния КС говорить о её возможном заражении компьютерными вирусми.

19. МЕТОД ВЫЯВЛЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ С ИСПОЛЬЗОВАНИЕМ МАТЕМАТИЧЕСКОГО АПАРАТА BDS-ТЕСТИРОВАНИЯ

к.т.н., проф. Гавриленко С.Ю., Челак В.В., НТУ "ХПИ",
к.т.н. Петров А.В. ХУ ВС им. И. Кожедуба , Харьков

В статье проведено исследование методов обнаружения злоумышленных атак на компьютерные и телекоммуникационные системы. Выявлена необходимость усовершенствования моделей информационных технологий и аргументированного выбора критериев оценки аномального поведения компьютерных и телекоммуникационных систем. Доказана целесообразность использования в качестве показателя аномального поведения компьютерной и телекоммуникационной системы характеристики джиттера значений BDS-теста, а критерием оценки – процентного отклонения приведенного показателя от выбранных в результате эксперимента значений. Приведена сравнительная характеристика BDS-теста с нестандартными функциями корреляций.

20. ПІДВИЩЕННЯ ЯКОСТІ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ВИКОРИСТАННЯ ОПЕРАЦІЙ ДОДАВАННЯ ЗА МОДУЛЕМ ДВА

Сисоєнко С.В., Миронюк Т. В., ЧДТУ, Черкаси

На основі проведення обчислювального експерименту було проведено перевірку гіпотези про підвищення якості псевдовипадкових послідовностей на основі операцій додавання за модулем два псевдовипадкових послідовностей з гіршими характеристиками.

Для проведення експерименту були вибрані двадцять чотири двох розрядні операції, які утворюють математичну групу. В процесі експерименту проводилось кодування двома випадковими не виродженими операціями, які входять до даної групи з послідуючим додаванням результатів кодування за модулем два. Додатково проводилася перевірка виродженості результату додавання за модулем 2. Оскільки вибрані операції утворюють повну математичну групу, то відсутність операції для оберненого перетворення свідчить про виродженість результатів перетворення.

За результатами експерименту встановлено, що додавання за модулем два результатів перетворення, підвищує якість псевдовипадкових послідовностей оскільки відсутній механізм оберненого перетворення.

21. ИССЛЕДОВАНИЕ ПРИНЦИПОВ РАБОТЫ АНТИВИРУСНОЙ СИСТЕМЫ

к.т.н., проф. Гавриленко С.Ю., Саенко Д.Н., НТУ "ХПИ", Харьков

В работе рассмотрены основные принципы работы антивирусной системы. Первая группа подходов и методов, включает поиск сигнатур, расчет контрольных сумм, вычисление коэффициентов "похожести", криптоанализ, эвристический анализ совокупностей разнообразных признаков. Вторая группа антивирусной защиты анализирует состояние компьютерной системы и детектирует вирусы в процессе их работы по характерной последовательности выполняемых действий. Цель работы - сформировать полную стуктуру антивирусной системы и выявить достоинства и недостатки наиболее распространенных методов антивирусной защиты.

22. ОЦІНКА ПРОПУСКНОЇ СПРОМОЖНОСТІ ПРИХОВАНОГО КАНАЛУ ЗВ'ЯЗКУ

д.т.н., проф. Кобозєва А.А., Ворнікова М.В., Шпортюк А.Г., ОНПУ, Одеса

У докладі пропонується метод оцінки величини пропускної спроможності прихованого каналу зв'язку, організованого за допомогою стеганографічного методу модифікації найменшого значущого біта. Як контейнер розглядається цифрове зображення. Основна ідея полягає в кількісній оцінці норми вектора збурення, що відбулося в результаті стеганоперетворення контейнера, високочастотних коефіцієнтів дискретного косинусного перетворення блоків матриці цифрового зображення-контейнера, отриманих шляхом стандартної розбивки. Отримання оцінки величини пропускної спроможності прихованого каналу зв'язку дасть при її використанні можливість підвищити ефективність стеганоаналізу з погляду не тільки детектування, але, головне, й декодування переданої інформації, що є надзвичайно актуальним у даний момент.

23. НОВЫЙ ПОДХОД К ОРГАНИЗАЦИИ ПРОВЕРКИ ЦЕЛОСТНОСТИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ, ОСНОВАННЫЙ НА МАТРИЧНОМ АНАЛИЗЕ

Бобок И.И., д.т.н., проф. Кобозева А.А., ОНПУ, Одесса

В докладе представлены основы нового общего подхода к организации проверки целостности цифровых изображений (ЦИ), базирующегося на мат-

ричном анализе. Определены, теоретически обоснованы и практически проверены новые свойства формальных параметров, определяющих ЦИ. Показано, что для большинства $l \times l$ – блоков матрицы оригинального изображения, полученных путем стандартного разбиения, угол между левым (правым) сингулярным вектором, отвечающим наибольшему сингулярному числу, и вектором, составленным из сингулярных чисел блока, определяется углом между *n*-оптимальным вектором $n^O = \left(1/\sqrt{l}\ ,..,\ 1/\sqrt{l}\right)^T \in R^l$ и первым вектором e_1 стандартного базиса пространства R^l. Установленная особенность нарушается для упомянутых формальных параметров в неоригинальном ЦИ. Это является показателем нарушения его целостности, в частности, показателем наличия внедренной при помощи стеганографических алгоритмов дополнительной информации, и может быть использовано как основа для разработки универсальных стеганоаналитических алгоритмов.

24. ВЗАЄМОЗВ'ЯЗКИ МІЖ ОПЕРАЦІЯМИ В МАТРИЧНИХ МОДЕЛЯХ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

к.т.н., доц. Бабенко В.Г., Лада Н.В.,ЧДЕУ, Черкаси, Лада С.В., ЧНУ ім. Б. Хмельницького, Черкаси

В доповіді представлені результати обчислювального експерименту з використання операцій додавання за модулем два та перестановки для реалізації матричних операцій криптоперетворення, здійснено поділ матричних моделей криптоперетворення на три групи за наявністю та типом перестановки в них: повного симетричного криптоперетворення, в яких послідовності шифрування і розшифрування співпадають для всієї групи операцій; частково несиметричного криптоперетворення, де послідовності шифрування і розшифрування не співпадають; умовно повного несиметричного криптоперетворення, в деяких окрім зміни операції, змінюється і матриця розшифрування. Виявлено, що взаємозв'язки між операціями, що застосовуються для криптографічного перетворення на основі матричних моделей, характеризуються циклічністю. Отримані цикли послідовності застосування операцій дозволяють будувати операції прямого та оберненого криптоперетворення в групі 2-розрядних матричних операцій з використанням запропонованих 2-операндних операцій.

25. АНАЛИЗ АТАК ТИПА ВНЕДРЕНИЯ SQL-КОДА

Коваль В.Р., ХНУРЭ, Харьков

В докладе рассмотрены особенности современных SQL-инъекций. Описаны основные принципы атак внедрения SQL-кода. Рассмотрены и проанализированы преимущества и недостатки атак типа внедрения SQL-кода. Опи-

саны основные способы защиты от этих атак. Проведен анализ современной тенденция SQL-инъекций, в ходе которого было выяснено, что многие организации страдают от этих атак, но не предотвращают их. Хакерские атаки с помощью SQL-инъекций происходят с большой регулярностью, и восстановление систем и файлов после этих инцидентов может быть дорогостоящим и неудобным.

26. УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ В КОРПОРАТИВНЫХ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ И СЕТЯХ СВЯЗИ

Кравчук П. В., ХНУРЭ, Харьков

Интерес к теме информационной безопасности и большое количество разнообразных публикаций по этой проблеме могут подвести к мысли, что основную угрозу конфиденциальным документам, финансовой информации представляют злоумышленники, работающие в Интернете, хакеры, почтовые вирусы, то есть всё, что называется hi-tech-угрозами. Таким образом, встает вопрос, что проще: осуществить взлом через Интернет или подкупить сотрудника организации? К сожалению, достаточно сложно собрать полную информацию по имевшим место утечкам и потере информации из-за понятной закрытости этой темы, и нежелания служб безопасности различных организаций оглашать негативные факты своей работы.

27 МОДИФІКАЦІЯ СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ, СТІЙКОГО ДО НАКЛАДАННЯ ШУМУ

Костирка О.В., Назаренко К.В., ЧІПБ ім. Героїв Чорнобиля Національного університету цивільного захисту України, Черкаси

У докладі представлена модифікація розробленого раніше одним з авторів стійкого до накладання різних шумів, найчастіше використовуваних при моделюванні активних атакуючих дій на стеганоповідомлення (гауссівського, мультиплікативного, пуассонівського), стеганографічного алгоритму, що здійснює вбудову додаткової інформації в просторовій області контейнера-зображення. Модифікація дозволяє, залишаючи стійкість алгоритму, яка кількісно оцінюється за допомогою коефіцієнту кореляції для вбудованої інформації, практично незмінною, зменшити спотворення контейнера, що виникає в результаті стеганоперетворення, і кількісно оцінюється за допомогою пікового відношення "сигнал-шум". Це дає можливість підвищити стійкість стеганоалгоритму до стеганоаналізу. Модифікований алгоритм має незначну обчислювальну складність: є поліноміальним ступеня 2. Характеристики алгоритму не залежать від формату (з втратами, без втрат) використовуваного зображення-контейнера.

28. СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ПРОВЕРКИ ПРОСТОТЫ ЧИСЕЛ

Денисов А.А., НАУ им. Н.Е. Жуковского "ХАИ", Харьков

В докладе рассмотрены различные алгоритмы проверки простоты чисел, из них часть была отобрана для реализации и более детального изучения и сравнения между собой. Для реализации были отобраны как детерминированные, так и вероятностные алгоритмы проверки простоты чисел, кроме того рассматривались также алгоритмы для проверки чисел Мерсена и Фибоначчи. Получены графические зависимости времени работы алгоритмов для чисел различной длины и сделаны выводы о качестве работы специализированных алгоритмов проверки простоты чисел.

29. ВИЗНАЧЕННЯ КІЛЬКІСНИХ ПОКАЗНИКІВ ПОРУШЕННЯ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ

Григоренко С.М., ОНПУ, Одеса

У докладі розглянуті кількісні показники цифрового зображення, що дозволяють відокремлювати оригінальне зображення від такого, цілісність якого була порушеною шляхом проведення операції клонування в умовах наступного збереження у форматі із втратами. Основним об'єктом аналізу є двовимірна матриця G, елементи якої відображають зв'язок між всіма можливими парами неспівпадаючих блоків матриці зображення. Встановлено, що кількість K елементів матриці G, значення яких дорівнює значенню її глобального мінімуму, різна у випадках наявності/відсутності клонування для переважної більшості протестованих цифрових зображень, а тому може використовуватися для розподілу оригінальних і змінених зображень при збереженні останніх з втратами (формат Jpeg) з коефіцієнтом якості $QF \in \{25, ..., 95\}$. Додаткових досліджень потребує випадок, коли $K=1$. Запропоновано процедуру проведення цих додаткових досліджень.

30. МЕТОД ПРОТИВОДЕЙСТВИЯ СЕТЕВЫМ УГРОЗАМ ДЛЯ САМООРГАНИЗУЮЩЕЙСЯ СИСТЕМЫ УПРАВЛЕНИЯ ТРАФИКОМ

к.т.н., доц. Угрин Д.И., Гаврилюк М.Н., Черновицкий факультет НТУ "ХПИ", Черновцы

Современные телекоммуникационные сети представляют собой модульные и открытые структуры. С одной стороны это позволяет динамически развиваться сетевым технологиям, а с другой предоставляет базу знаний для проведения злоумышленных действий. Современные средства защиты информации во многом имеют "жесткую" логику, предоставляющую злоумышленникам действенные алгоритмы их обхода или взлома.

В докладе представлен метод противодействия сетевым угрозам, который является основой самоорганизующейся системы управления трафиком, обеспечивающей информационную безопасность локальной вычислительной сети, обладающей свойствами динамической адаптации, оптимизации, автономности с пресечением возможности прогнозирования стратегии реагирования на атаки. Разработанная самоорганизующаяся система управления трафиком обладает высокими показателями отказоустойчивости, предотвращает перегрузку системы, оставляя до 30% системных ресурсов и пропускной способности сети.

31. ОЦЕНКА ТЕКУЩЕГО СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ДАННЫХ В ОБЛАЧНЫХ ХРАНИЛИЩАХ

Саенко А.А., ХНУРЭ, Харьков

В последнее время облачные вычисления становятся всё более востребованными, однако многие компании, так же как и частные лица считают облачные хранилища непроверенными и, как следствие, небезопасными. В работе определены показатели надежности хранения данных, разработана модель оценки рисков информационной безопасности и на её основе проведена оценка текущего состояния защищенности данных в облачных хранилищах. Получены результаты, которые показывают зависимость потерь заинтересованной стороны от реализации угрозы.

32. СРЕДА МОДЕЛИРОВАНИЯ ДЛЯ ИССЛЕДОВАНИЯ ВОЗМОЖНОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ GRID- И CLOUD-СИСТЕМ

к.т.н., проф. Заполовский М.Й., к.т.н., доц. Мезенцев Н.В. НТУ "ХПИ", Харьков

В последнее время все большее внимание уделяется программным средствам обеспечения безопасности ресурсов больших распределенных информационно-вычислительных систем. Несмотря на то, что для Grid- и Cloud-систем создано значительное число разноуровневых средств такого назначения, обеспечение их надежной защиты является сложной, трудоемкой и ресурсозатратной задачей. Для ее эффективного решения необходимо оценивать и корректировать уровень защищенности подобных систем на разных архитектурных уровнях их реализации. Поэтому разработка и реализация программной среды для гибридного моделирования Grid- и Cloud-систем является актуальной.

Представленная в докладе программная среда позволяет эффективно представить и опробовать сразу несколько уровней системы при небольших затратах на сам процесс исследования.

33. МЕТОД ПРОГНОЗИРОВАНИЯ ПРИ ПЕРЕДАЧЕ МУЛЬТИМЕДИЙНЫХ ДАННЫХ В СИСТЕМАХ СВЯТИ

Горюшкина А.Е., Горюшкина И.Н., НТУ "ХПИ", Харьков

Проведенные исследования показали, что при проектировании телекоммуникационных сетей для оптимизации работы отдельных узлов и обеспечения требуемого качества обслуживания требуются подробные данные о многих параметрах отрасли (количестве соединительных линий, пропускной способности каналов связи и т.д.), а также варианты схем распределения информационного потока в сети. Данные показатели определяются на основе многих предпроектных материалов. Отсутствие таких данных может привести к неэффективному использованию ресурсов отдельных узлов и телекоммуникационной сети в целом, перегрузке отдельных сегментов сети, а в отдельных случаях и локальным сбоям в работе. Прогнозирование нагрузки относится к такому классу задач, где зависимость между входными и выходными переменными сложна, а нахождение закономерностей в больших объёмах данных требует нетривиальных алгоритмов и занимает много времени.

Предложенный в докладе подход был применен для прогнозирования интенсивности потока данных двух аспектов: фрактальной интерполяции и фрактальной экстраполяции. По результатам исследования средняя относительная ошибки составила всего 2.303% и 2.296%, в случае шести опорных точек для полного набора прогнозных данных.

34. АНАЛИТИЧЕСКИЙ ОБЗОР МЕТОДОВ ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ В ИНТЕРНЕТЕ

Заикин В.А., ХНУРЭ, Харьков

Обеспечение достаточно высокой анонимности субъекта при его взаимодействии с адресатом в информационно-вычислительных сетях относится к числу сложных проблем современных информационных технологий. В работе рассмотрено свойство анонимности с технической точки зрения, когда потеря конфиденциальности связана с программно-аппаратными средствами, а не с социальным аспектом, когда, например, пользователь сам, осознанно или нет, рассказывает о себе под воздействием методов социальной инженерии. Цель работы – выявить достоинства и недостатки наиболее распространенных методов обеспечения анонимности пользователя.

35. МЕТОД ДИНАМИЧЕСКОЙ ОЦЕНКИ СОСТОЯНИЯ UMTS-КАНАЛА УПРАВЛЕНИЯ МОБИЛЬНЫМИ ОБЪЕКТАМИ

Петрук В.В., ХНУРЭ, Харьков

Предлагаемый метод оценки состояния UMTS-канала управления мобильными объектами основан на выявленной и подтвержденной эксперимен-

тально корреляции между параметрами радиоканала и показателями процесса информационного обмена. Предложена вероятностная модель позволяющая получить вероятность изменения состояния канала информационного обмена, и определены количественные значения ее параметров. Этот метод может быть использован в алгоритмах управления мобильными объектами и роботами, а также при оперативном планировании использования системой управления канала передачи данных.

36. САМОДИАГНОСТИРОВАНИЕ АППАРАТНЫХ МОДУЛЕЙ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

Караман Д. Г., НТУ "ХПИ", Харьков

В докладе представлены методы решения проблемы высокой чувствительности аппаратных реализаций средств криптографической защиты данных к сбоям и ошибкам, которые возникают в процессе работы. Предложенные методы призваны не только повысить надежность и производительность криптографических средств, но и обеспечить противостояние новому классу атак, основанных на искусственном вызове сбоев в процессе функционировании устройства, существенно упрощающих взлом атакуемого устройства. Рассмотрены практические примеры реализации предлагаемых методов. Проведенные моделирования и анализ показывают высокую эффективность предлагаемых методов в оперативном обнаружении и нейтрализации сбоев в процессе шифрования.

37. ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕЦП, ЩО РЕАЛІЗОВАНІ В ПОЛЯХ ТА ГРУПІ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ

Даас Т.І., ХНУРЕ, Харків

В доповіді розглянуті основні алгоритми формування електронного цифрового підпису. Проаналізовані основні вимоги до ЕЦП, та відповідність розглянутих алгоритмів цим вимогам. Було наведено специфічні атаки на кожен алгоритм формування підпису, порівняна ефективність цих атак на інші алгоритми та запропоновані вдосконалення для протидії цим атакам. Проаналізувавши усі особливості, були запропоновані найбільш придатні алгоритми для кожного з рівнів захищеності, які висуває сучасний інформаційний світ для обробки, передавання та збереження будь-якого виду інформації. В ході роботи були розглянуті різні платформи та ефективність реалізації алгоритмів ЕЦП на кожній з них. Також було проаналізовано кількість основних операцій, які використовуються в криптопримітивах. Зроблено висновки щодо обчислювальної складності кожного з алгоритмів на основних платформах.

38. МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Зінченко В.С., ХНУРЭ, Харьков

На сегодняшний день существуют множество методов и средств для "обхода" систем защиты информационных систем (ИС). Их количество и многообразие растет из года в год, что является причиной для тревоги. Изменить ситуацию можно путем разработки новых подходов к обеспечению безопасности ИС, способных обеспечить надежную защиту от современных угроз. Особое внимание в настоящее время уделяется защите персональных данных субъектов. Это направление является одним из приоритетных в обеспечении информационной безопасности любой компании. Цель работы – разработка методики оценки эффективности системы защиты персональных данных за счет использования методов обработки трудно формализуемых данных предметной области.

39. АНАЛИЗ СЕТЕВОЙ АТАКИ IP-SPOOFING

Скибенко Н.С., ХНУРЭ, Харьков

В докладе рассмотрены особенности атаки типа IP-spoofing на корпоративные сети. Предложены методы защиты сетей от данной атаки, среди которых наиболее эффективными являються: проверка адреса отправителя (Sourse Address Verification), сопоставление MAC-адреса (Ethernet кадр) и IP-адреса (заголовок протокола IP) отправителя. В докладе были приведены примеры сервисов уязвимых к атаки IP-spoofing, среди которых: RPC (удаленный вызов процедур), X Windows System, r-службы и службы, которые используют адрес аутентификацию IP.

Проведенный анализ показал, что данная атака является достаточно опасной, учитывая большое число её модификаций, и соответственно проблема защиты сетей от атаки типа IP-spoofing является актуальной в наши дни.

40. МЕТОДЫ БОРЬБЫ С ВРЕДОНОСНЫМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

Шевченко В.И., ХНУРЭ, Харьков

В ходе работы были исследованы и проанализированы основные методы борьбы с вредоносным программным обеспечением, а также рассмотрены проблемы, связанные с защитой сетевой инфраструктуры закрытого предприятия. В связи со спецификой распространения вируса, в ходе работы были сделаны выводы о необходимости включения в пакет поставки предустановленный набор утилит для полного обслуживания оборудования, чтобы исключить использование внешних электронных носителей информации, а так

же существует необходимость использования замкнутых локальных сетей без доступа в интернет.

41. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ НУЛЕВЫХ ЗНАНИЙ

Уманская Ю.О., ХНУРЭ, Харьков

В докладе были рассмотрены следующие протоколы нулевого разглашения: протокол Шнорра, протокол Фиата-Шамира, протокол Гиллоу-Кискатера и протокол с нулевым разглашением способом преобразования в конечном поле Галуа. Исследованы возможные модели атак и способы защиты. Изучены уязвимости данных интерактивных протоколов. Выполнено сравнение протоколов на основе следующие параметров: коммуникационные затраты, вычислительные затраты, требования к памяти, гарантии безопасности, наличие доверенного центра. В результате проведения сравнительного анализа данных протоколов было выявлено что протокол Гуилоу – Кискатера предпочтительнее протокола Фиата-Шамира и его модификации относительно коммуникационных затрат и гарантий безопасности. Однако по вычислительным затратам он проигрывает, так как больше предвычислений, доказывающий и проверяющий выполняют умножение и возведение в степень больших чисел.

42. ПЕРСПЕКТИВЫ РАЗВИТИЯ АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Деревянко А.А., ХНУРЭ, Харьков

Разработке и производству современных средств защиты от несанкционированного доступа (НСД) к информации в ОКБ САПР предшествовало выполнение научно-исследовательских и опытно-конструкторских работ в этой области. Большинство разработчиков на первоначальном этапе были сосредоточены на создании только программного обеспечения, реализующего функции защиты в автоматизированных системах, что не может гарантировать надежной защищённости автоматизированных систем от НСД к информации. К примеру, проверка целостности программной среды, осуществляемая какой-либо другой программой, находящейся на одном носителе с проверяемыми объектами, не может гарантировать правильности проводимых процедур. Необходимо обеспечить достоверность самой программы проверки целостности, а только затем выполнение ее контрольных процедур. Таким образом, это привело к осознанию необходимости использования в системах защиты информации от НСД аппаратных средств со встроенными процедурами контроля целостности программ и данных, идентификации и аутентификации, регистрации и учета.

43. ПАРОЛЬНАЯ ЗАЩИТА ПОЧТОВЫХ СЕРВИСОВ

Джурик О.В., ХНУРЭ, Харьков

В докладе рассмотрена подсистема аутентификации. Несмотря на неуклонное развитие механизмов информационной безопасности, наиболее используемым средством аутентификации является пароль. Основной уязвимостью такого механизма защиты считается выбор не стойкого пароля. В 2014-2015 годах произошел ряд утечек парольних баз крупних интернет-компаний, что позволило провести исследование стойкости реальних паролей. Следует констатировать, что за прошедшее время защита парольних систем не сильно продвинулась вперед, в основном видна тендеция роста требований к интерфейсу вводу пароля. При этом до сих пор стоит вопрос, какие пароли можно считать стойкими, а какие нет.

В работе приводятся примеры оценки парольних систем, а также проведен анализ утекших паролей на предмет их стойкости по разработанным требованиям. Проверка стойкости проводилась при помощи использования метрик(показателей стойкости паролей).

Данные метрики являлись основой для формулирования объективных требований к стойкости парольной системы.

44. УГРОЗЫ БЕЗОПАСНОСТИ, СВЯЗАННЫЕ С МОБИЛЬНЫМИ УСТРОЙСТВАМИ

Масленникова А.О., ХНУРЭ, Харьков

В докладе рассмотрены угрозы информационной безопасности, связанные с эксплуатацией мобильных устройств. Проанализированы основные свойства мобильных устройств, которые определяют их слабые места с точки зрения защиты информации, а также условия эксплуатации данных устройств, создающие возможности для нарушения конфиденциальности, целостности и доступности информации. Определены зависимости между указанными факторами и наиболее вероятными специфичными угрозами безопасности информации.

Проведенный анализ показал, что мобильные устройства практически при любых условиях создают дополнительные угрозы для информационной безопасности, что представляет опасность, как для пользователей, так и для компаний, сотрудники которых осуществляют эксплуатацию устройств.

Наилучшим условием для минимизации угроз является использование доверенного устройства на контролируемой территории при отсутствии доступа к информационной системе.

45. УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ В КОРПОРАТИВНЫХ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ И СЕТЯХ СВЯЗИ

Сидоров В.В., ХНУРЭ, Харьков

Интерес к теме информационной безопасности и большое количество разнообразных публикаций по этой проблеме могут подвести к мысли, что основную угрозу конфиденциальным документам, финансовой информации представляют злоумышленники, работающие в Интернете, хакеры, почтовые вирусы, то есть всё, что называется hi-tech-угрозами. Таким образом, встает вопрос, что проще: осуществить взлом через Интернет или подкупить сотрудника организации? К сожалению, достаточно сложно собрать полную информацию по имевшим место утечкам и потере информации из-за понятной закрытости этой темы, и нежелания служб безопасности различных организаций оглашать негативные факты своей работы.

46. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ВИДЫ УГРОЗ

Гапон А.А., ХНУРЭ, Харьков

В докладе рассмотрены угрозы информационной безопасности. Проанализированы основные характеристики и принципы информационной безопасности, а также воздействия естественного и искусственного характера, которые могут нанести ущерб пользователю, устройства, которые определяют их слабые места с точки зрения защиты информации, а также условия эксплуатации данных устройств, создающие возможности для нарушения конфиденциальности, целостности, доступности и достоверности информации. Задача обеспечения информационной безопасности подразумевает реализацию многоплановых и комплексных мер по предотвращению и отслеживанию несанкционированного доступа неавторизованных лиц, а также действий, предупреждающих неправомерное использование, повреждение, искажение, копирование, блокирование информации. Различают естественные и искусственные угрозы, по степени преднамеренности проявления, угрозы делят на случайные и преднамеренные. Угрозы могут быть активного и пассивного воздействия. Часто используют специальные вердоносные программы.

47. АНАЛИЗ СТРУКТУРЫ НОВОГО ВИРУСА REGIN

Кравчук П.В., ХНУРЭ, Харьков

В докладе была рассмотрена архитектура вируса REGIN, его возможности и способы обнаружения. Проанализированы уязвимости, которые использует этот вирус. Было установлено, что REGIN является невероятно сложным компонентом программы, отличающийся гибкостью своих возможностей в зависимости от цели, для атаки на которую его готовят. Этот вирус

поражает компьютеры под управлением операционной системы Microsoft Windows. Проведенный анализ показал, что в его основе лежит особая структура, разработанная для обеспечения операций длительного скрытого сбора информации. REGIN надежно шифрует следы своей работы и имеет множество таких возможностей, как анализ электронной почты, экранных снимков, перехват сетевого трафика и т.д. Многие компоненты вируса до сих пор не были открыты и полный список его возможностей неизвестен.

48. АНАЛІЗ МЕТОДІВ КРИПТОАНАЛІЗУ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

Вітюк К.Ю., ХНУРЭ, Харьков

У доповіді був проведений аналіз різних алгоритмів створення симетричних блокових шифрів, а також розглянуті деякі методи криптоаналізу блокових симетричних шифів. Більш детально був розглянутий диференціальний метод криптоаналізу і його застосування до шифру DES. Диференціальний криптоаналіз – метод, який грунтується на вивченні впливу певних відмінностей у відкритих (плайн-текстових) парах блоків інформації на відмінності результуючих зашифрованих пар блоків. Окрім того, в доповіді представлений порівняльний аналіз диференціального методу з іншими і зроблені висновки щодо доцільності його використання.

49. ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КЛІНІЧНОГО МОНІТОРИНГУ СІМЕЙНОГО ЛІКАРЯ

Сітнікова О.О., НТУ «ХПІ», Харків

Розглянуто проблеми, пов’язані зі збором та обробкою медико-біологічних параметрів пацієнтів, з точки зору вирішення задачі клінічного моніторингу. Відповідно до сучасних досліджень в області електронної медицини, найбільш перспективною є концепція HealthGrid, яка являє собою Grid-інфраструктуру, орієнтовану на вирішення медичних завдань. HealthGrid можна використовувати в двох аспектах: для індивідуальних потреб пацієнта і для епідеміологічного аналізу. Перший підхід забезпечує доступ до клінічних даних пацієнта для вирішення поточних проблем. Другий підхід дозволяє використовувати медичну інформацію для пошуку залежностей між антропологічними даними, факторами ризику, симптомами, захворюваннями. Технологія HealthGrid інфраструктури дозволяє розподілено обробляти дані пацієнтів різних лікарів із різних медичних закладів.

Запропоновано поєднати можливості сучасних портативних та вбудованих медичних приладів, математичного забезпечення систем медичного діагностування та переваги колаборативних рекомендаційних систем у межах HealthGrid архітектури. Такий підхід підвищує ефективність та якість систем ППР сімейного лікаря за рахунок автоматизації збору первинних медичних

даних пацієнта, обробки даних клінічного моніторингу та надання рекомендацій з урахуванням статистичної на наукової медичної інформації.

50. АНАЛИЗ МЕТОДОВ КРИПТОАНАЛИЗА ПОТОКОВЫХ СИММЕТРИЧНЫХ ШИФРОВ

Биличенко Д.Г., ХНУРЭ, Харьков

В докладе описаны различные методы криптоанализа классических потоковых симметричных шифров. Возможные атаки на данный вид шифров. В рамках доклада была дана краткая характеристика потоковым криптографическим алгоритмам, а так же были проанализированы возможные криптографические атаки на него. Проанализировав методы криптоанализа, были сделаны выводы, занесенные в сравнительные таблицы. В процессе работы определены наиболее удобные алгоритмы для шифрования данных в зависимости от поставленных задач.

51. АНАЛИЗ ПРОТОКОЛА IPv6, И ЕГО УЯЗВИМОСТИ

Панченко С.А., ХНУРЭ, Харьков

В докладе был рассмотрен протокол IPv6 и виды возможных атак на него. Протокол IPv6 объединяет сегменты сети в единую сеть, обеспечивая доставку пакетов данных между любыми узлами сети через произвольное число промежуточных узлов. В настоящее время протокол IPv6 уже используется в нескольких тысячах сетей по всему миру но пока ещё не получил столь широкого распространения в Интернете, как IPv4. Данный протокол отличается от предшественника использованием протокола IPSec, который позволяет шифровать любые данные без необходимости какой-либо поддержки со стороны прикладного ПО. Введение в протоколе IPv6 поля «Метка потока» позволяет значительно упростить процедуру маршрутизации однородного потока пакетов. В ходе данной работы были проанализированы виды возможных атак на IPv6, такие как: DDOS-атака, SLAAC-атака, атака Rogue RA. В результате были изучены особенности данного протокола и его известные уязвимости, что дало возможность утверждать об уровне надёжности использования данного протокола.

52. ПОЛЬЗОВАТЕЛИ ПОД УГРОЗОЙ: КЛИКДЖЕКИНГ

Дмітрієв К.І., ХНУРЭ, Харьков

Мы все сильно зависим от интернета и гаджетов, при этом делаем себя крайне уязвимыми для мошенников, которые обитают в сети. И с каждым годом у киберпреступников появляется все больше возможностей атаковать пользователей. Одна из главных опасностей для украинских пользователей интернета в 2015 году – кража денег с банковских счетов. Большое распро-

странение в 2015 году получил кликджекинг – механизм обмана, при котором пользователь перенаправляется на вредоносную страницу при клике на ссылку. Чаще всего этот механизм используется в соцсетях. Еще одна проблема, которая беспокоит пользователей в 2015 году – неприкосновенность их частной жизни. Не секрет, что все, что не запрещено, в интернете по умолчанию разрешено. И если никак не ограждать свою частную жизнь в интернете, различные сервисы могут беспрепятственно собирать информацию о пользователях и использовать её для рекламы, рассылок и так далее.

53. СРАВНИТЕЛЬНЫЙ АНАЛИЗ КИБЕРАТАК

Ратий А.О., ХНУРЭ, Харьков

В докладе были рассмотрены следующие типы атак: социальная инженерия, инфицирование компьютеров вредоносным программным обеспечением, инъекции кода и сетевая разведка. Исследованы возможные способы предотвращения таких атак и защиты. Изучены уязвимости основных протоколов к данным атакам. В результате проведения сравнительного анализа данных атак было выявлено, что методы социальной инженерии более эффективны, чем инфицирование вредоносным программным обеспечением и подобные методы. Повсеместное использование мобильных устройств работниками компаний предоставляет злоумышленникам больше возможностей для доступа к корпоративным системам. Была замечена тенденция роста атак направленных на хищение личности. В подавляющем большинстве случаев злоумышленники получали доступ к информации пользуясь некомпетентностью или небрежностью персонала на рабочем месте.

54. ПАРОЛЬНАЯ ЗАЩИТА ПОЧТОВЫХ СЕРВИСОВ

Задеренко Д.С., ХНУРЭ, Харьков

В докладе рассмотрена подсистема вэб-аутентификации. Наиболее часто используемой аутентификации является пароль. Кроме него есть также способ через СМС или через личный звонок. Это называется аутентификауией второго уровня. Такие системы, как банковские, используют ее. Однако большинство систем используют пароль. Основной уязвимостью такого механизма защиты считается выбор не качественного пароля. В 2014-2015 годах произошел ряд утечек парольних баз крупних интернет-компаний, что позволило провести исследование стойкости реальних паролей. Следует констатировать, что за прошедшее время защита парольних систем не сильно продвинулась вперед, в основном видна тендеция роста требований к интерфейсу вводу пароля. Учитывая то, что большинтсво систем написано на JS, является не ясным тот факт, то они уязвимы к атакам на определенные страницы. При этом до сих пор стоит вопрос, какие пароли можно считать стойкими, а какие нет. Пприводятся примеры оценки парольних систем, а также проведен анализ паролей на предмет их стойкости по разработанным требо-

ваниям. Проверка стойкости проводилась при помощи использования метрик (показателей стойкости паролей). Данные метрики являлись основой для формулирования объективных требований к стойкости парольной системы.

55. АНАЛИЗ ПРОТОКОЛА SSL И ЕГО УЯЗВИМОСТИ

Белотел В.А., ХНУРЭ, Харьков

В докладе рассматривается криптографический протокол SSL и виды возможных атак на него. Протокол SSL обеспечивает согласование алгоритмов и обмен ключами шифрования, а так же используется для защиты данных при их перессылке по сетям. SSL использует асимметричную криптографию для аутентификации ключей обмена и симметричный шифр для сохранения конфиденциальности. Также протокол использует среду с несколькими слоями, что обеспечивает безопасность обмена информацией. Помимо этого были проанализированы виды возможных атак на SSL, такие как: атака по словарю, атака отражением, атака протокола рукопожатия, взлом SSL соединений внутри ЦОД, BEAST атака, RC4 атака, атака «встреча посередине», THC-SSL-DOS и SSLstrip. Были изучены особенности данного протокола и его известные уязвимости, что дало возможность утверждать об уровне надёжности использования данного протокола.

56. АНАЛИЗ ОСОБЕНОСТЕЙ ВОЗМОЖНЫХ DOS-АТАК И ЗАЩИТА ОТ НИХ

Евгеньев А.М., ХНУРЭ, Харьков

В докладе рассмотрены и проанализированы, в каких сферах и с какой целью чаще всего используются DOS-атаки, особенности возможных DOS-атак, также, были рассмотрены оптимальные способы защиты от этих угроз, как общие, так и индивидуальные для каждой атаки. Были рассмотрены такие DOS-атаки как: HTTP-флуд и ping-флуд, ICMP-флуд, UDP-флуд, переполнение сервера лог-файлами, переполнение буфера и др. На основе рассмотренных угроз предложены методы защиты от них, и сформированы универсальные советы для того, что бы система была готова к возможной DOS-атаке. Анализ показал, что больше всего страдает правительственная сфера, интернет-магазины, и FOREX, самой распространенной атакой является ping-флуд, так как она не требует большого количества знаний и умений от нарушителя.

57. АНАЛИЗ АТАК ТИПА МЕЖСАЙТОВЫЙ СКРИПТИНГ И СРЕДСТВ ЗАЩИТЫ ОТ НИХ

Курочка А.Ю., ХНУРЭ, Харьков

В докладе рассмотрены атаки типа межсайтовый скриптинг (XSS-атаки), проанализирована их классификация (по вектору, по каналам внедрения скрипта, по способу воздействия). Реализация данных атак злоумышленником

может привести к таким последствиям: кража аккаунта, получение доступа к защищенным данным, повреждение веб-приложения, слежение за посещением сайта пользователем, получение бесплатного доступа к платному контенту. Как пример, слабые места в системе безопастности сайта могут позволить хакерам получать сведения о кредитных картах и пользователях в результате чего злоумышленики могут осуществлять денежные переводы на свое имя. XSS-атаки являются очень опасными и находятся на третьем месте в рейтинге ключевых рисков web-приложений согласно OWASP 2013. Также были рассмотрены реализации данных атак на тестовые сайты, и в результате проанализированы средства защиты (как со стороны сервера, так и со стороны клиента) от таких угроз.

58. SECURITY SMART TOYS FOR CHILDREN

Levchenko D.D. National Aerospace University named after N.E. Zhukovsky "KhAI", Kharkov

The report examined the existing types of smart toys IoT (Internet of things) for children and information transmission methods from their parents to electronic devices (tablets, smartphones, laptops and other). Analyzed data security levels. Research has shown that not all smart toys have the necessary protection and are vulnerable to hackers. Attackers could also access to personal details like the kid's name, birth date, gender, and language were also available, along with the current status of the toy (if the child was playing with it), delete toy profiles and switch toys from one account to the other, changing their behavior and confusing the children with wrong responses. There is a solution to this problem – security testing API. It allows protecting services and consumers against the most common security vulnerabilities by using a complement of prebuilt tests and scans.

59. БЕЗПЕКА SCADA СИСТЕМИ ВОДООЧИСНИХ СПОРУД

к.т.н., доц. Ляшенко О.С., Цяпа О.В., Олефіренко І.О., ХНУРЕ, Харків

В доповіді розглянута робота SCADA систем, які мають ієрархічну структуру, щонайменше, два рівні контролю: регулюючого та диспетчерського контролю. Проведена оцінка загроз безпеки SCADA системи водоочисними спорудами. Кібератаки можна класифікувати таким чином, або атаки на порушення цілосності даних, які передаться в системі, або атаки на відмому обслуговуванні обладнення (DoS). Цілісність пакетів даних з датчиків і керуючих пристроїв відноситься до їх надійності, а відсутність цілісності може привести до отримання недостовірних даних. Кібератаки на SCADA систему інфраструктури водоочисних споруд може привести до часткової або повної втрати експлуатаційних характеристик, таких як стабільність роботи замкнутого контуру, безпеки по відношенню до надмірної доливання або втрати продуктивності. В роботі розроблені моделі різноманітних атак та методи визначення оцінки загрози для SCADA системи водоочисних споруд.

СЕКЦІЯ 2
ОРГАНІЗАЦІЙНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Керівники секції: д.т.н., проф. Кучук Г.А., ХУ ПС ім. І.Кожедуба, Харків

Секретар секції: к.т.н., проф. Гавриленко С.Ю., НТУ "ХПІ", Харків

1. НАХОЖДЕНИЕ МЕСТОРАСПОЛОЖЕНИЯ ПРОСТЫХ ЧИСЕЛ

к.т.н., доц. Певнев В.Я., НАУ им. Н.Е., Жуковского "ХАИ", Харьков

В докладе рассмотрена проблема распределения простых чисел. Приведены теоремы, с помощью которых возможно нахождение простых чисел. Представлены результаты эксперимента, показывающие эффективность предлагаемого метода. Показаны различные подходы, определяющие возможное месторасположение простых чисел. Сформулированы дальнейшие пути усовершенствования предложенного подхода, позволяющие значительно ускорить процесс нахождения простых чисел большого размера. Теоретические выкладки иллюстрируются практическими примерами.

2. ТЕОРЕТИЧНІ ЗАСАДИ ТРАНСФОРМАЦІЇ СТРУКТУРИ ДАНИХ, ЩО ЗАХИЩАЮТЬСЯ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

к.т.н., доц. Возна Н.Я., ТНЕУ, Тернопіль

В доповіді викладені теоретичні засади трансформації структури даних, що захищаються від несанкціонованого доступу шляхом формалізації процесів їх структуризації в одномірному, двомірному та трьохмірному сигнальних просторах. Показано, що у процесі трансформації даних, що захищаються від несанкціонованого доступу відбувається зміна структурної складності та ентропійної інформативності, запропоновані критерії оцінки структурної складності незахищених та зашифрованих даних на основі атрибутів двомірного Хеммінгового простору. Розглянуті питання сумісної критеріальної оцінки неповнофункціональних та повнофункціональних компонентів даних, що захищаються від несанкціонованого доступу. Приведені приклади трансформації структури даних у процесах їх шифрування та захисту.

3. ИССЛЕДОВАНИЕ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ НА РЕГИСТРАХ СДВИГА С ОБРАТНОЙ СВЯЗЬЮ

Фролов В.В., к.т.н., доц. Певнев. В.Я., НАУ им. Н.Е. Жуковского "ХАИ", Харьков

В докладе рассмотрены особенности реализации ГПСЧ на регистрах сдвига, результаты анализа криптостойкости генератора на основе тестиро-

вание его статистических свойств. Улучшение статистических свойств ГПСЧ достигается за счет использования операции сложения по модулю 2 генерируемых битов двух регистров различной разрядности. Последующее тестирование выходной последовательности полученной при сложении, дало более случайную статистику. Также для анализа криптостойкости алгоритма генерации были проведены попытки получить структуру регистра по выходной последовательности. Криптоанализ на обычном и модифицируемом регистре дал различный результат. В то время как обычный алгоритм, возможно, скомпрометировать, зная 2n битов, для спряженного генератора стандартные методы анализа ГПСЧ на регистрах сдвига не работают.

4. АНАЛИЗ МОДИФИКАЦИИ КОНГРУЭНТНОГО ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Фролов О.В., к.т.н., доц. Певнев. В.Я., НАУ им. Н.Е. Жуковского "ХАИ", Харьков

В докладе рассмотрены особенности реализации конгруэнтного ГПСЧ. Для повышения криптостойкости генератора предложена следующая модификация: перевод сгенерированных последовательностей в двоичную систему счисления и побитовое сложение результатов двух параллельно работающих конгруэнтных ГПСЧ. Требования к генераторам - они должны быть не синхронизированы и иметь разные размеры генерируемой последовательности. Для определения криптостойкости генератора использовалась модель оценки на основе тестов NIST. Результаты проведенного анализа показывают, что криптостойкость данной модификации конгруэнтного ГПСЧ более высокая, по сравнению с классической реализации алгоритма.

5. ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ ДАНИХ В ІНТЕРАКТИВНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

к.т.н., доц. Пітух І.Р., ТНЕУ, Тернопіль

В доповіді виконаний аналіз архітектур та інформаційних технологій організації руху даних в інтерактивних комп'ютерних системах. Викладені теоретичні основи критеріїв інтерактивної взаємодії різних компонентів інтерактивних систем. Обгрунтовані методи кібернетичного захисту інформаційних даних, які формуються в процесі моніторингу об'єктів управління вибухонебезпечного, екологонебезпечного та стратегічного значення. Особливу увагу приділено методам захисту інформаційних потоків, які представляють команди інтерактивного управління розподіленими об'єктами захищеними від несанкціонованого доступу та перехоплення ініціативи управління об'єктом.

6. ПОСТРОЕНИЕ ГЕНЕРАТОРА ПРОСТЫХ ЧИСЕЛ

к.т.н., доц. Певнев В.Я., Радченко Н.В., НАУ им. Н.Е. Жуковского "ХАИ", Харьков

В докладе рассмотрены проблема нахождения и проверки больших простых чисел. Сложность задачи нахождения простых чисел многократно возросла ввиду того, что необходимо находить числа большого размера. При работе с такими цифрами задача нахождения простых чисел стала соизмеримой по сложности с задачей факторизации. Проанализированы существующие способы поучения простых чисел. Из результатов проведенного анализа, можно сделать вывод, что самым большим недостатком большинства методов построения ПЧ то, что все они хорошо работают на относительно небольших числах. Предлагается подход к построению больших простых чисел путем обнаружения возможных мест расположения на числовой оси.

7. АНАЛІЗ СУЧАСНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ІТ-СИСТЕМАХ

к.т.н., проф. Скородєлов В.В., Серпокрилов О.А., НТУ "ХПІ", Харків

Захист даних являється сьогодні однією з головних задач при розробці різних ІТ-систем. Існують різноманітні способи захисту інформації але кожний з них разом з перевагами має недоліки. Тому необхідно постійно вдосконалювати методи захисту інформації для того щоб забезпечити їх відповідність сучасним критеріям безпеки.

В роботі аналізуються програмні, апаратні та програмно-апаратні засоби захисту інформації в ІТ-системах. Визначаються їх основні відмінності, переваги та недоліки. Показуються переваги апаратно-програмних засобів по порівнянню з іншими. Розглядаються різні варіанти реалізації апаратної частини засобів захисту даних з використанням криптографічних процесорів, мікроконтролерів з криптографічними співпроцесорами та ПЛІС, в тому числі з архітектурою FPGA. Аналізуються можливі варіанти злому таких засобів за допомогою так званих "непрямих атак" та пропонуються методи захисту від них.

8. ЗАХИСТ ПЕРСОНАЛЬНИХ КОМП'ЮТЕРІВ ВІД КЕЙЛОГЕРІВ (КЛАВІАТУРНИХ ШПИГУНІВ)

к.т.н., проф. Скородєлов В.В., Стасюк С.І., НТУ "ХПІ", Харків

Програми-шпигуни та апаратні пристрої-кейлогери, які призначені для прихованого стеження за діяльністю користувачів персональних комп'ютерів, одержали в останній час дуже широке розповсюдження. Вони являються однією з найбільш актуальних проблем ІТ-безпеки. Більшість спе-

ціалістів рахують, що в майбутньому цей вид загроз стане самим небезпечним. Тому захист від даного виду загроз стає настільки актуальним.

В роботі аналізуються шляхи витоку інформації в персональних комп'ютерах а також різні типи апаратних та програмних клавіатурних шпигунів. Розглядаються особливості їх установки та шляхи проникнення в персональні комп'ютери. Пропонуються методи пошуку та протидії програмам–шпигунам та апаратним–кейлогерам. Наводяться приклади розробки програмних компонентів для захисту персональних комп'ютерів від клавіатурних шпигунів.

9. РАЗРАБОТКА АНТИВИРУСНОЙ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ НА БАЗЕ ГИПЕРВИЗОРА С ИММУНОПОДОБНЫМ РАСПОЗНАВАНИЕМ

к.т.н., проф. Гавриленко С.Ю, д.т.н., с.н.с. Семенов С.Г., Шевердин И.В., НТУ "ХПИ", Харьков

В докладе рассмотрено построение антивирусной программной системы, которая основывается на математической модели человеческого иммунитета для формирования самообучаемого принципа обнаружения и удаления вирусной угрозы. Система объединяется в коллаборацию горизонтально масштабируемых систем и формирует целостный организм. Результатом работы является формирование облачной базы данных поведения системы. В системе учтены возможности потери информации и разработаны механизмы нивелирования системных отказов и восстановления данных на основе произошедших изменений в системе. Использование аппаратной виртуализации и выделенного ядра антивирусной системы, позволяет избежать внешнего и внутреннего влияния на операционные системы.

10. ОЦЕНКА БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ, ОСНОВАННЫХ НА ТЕХНОЛОГИИ FPGA

д.т.н., проф. Рубан И.В., к.т.н., доц. Коваленко А.А., ХНУРЭ, Харьков; д.т.н., проф. Кучук Г.А., ХУ ВС им. И. Кожедуба, Харьков

В докладе представлен подход к оценке безопасности компьютерных систем, в том числе критического применения. Такой подход применим к разнообразным комплексным системам, в том числе основанным на технологии FPGA. Изложены и проанализированы основные этапы, включая анализ и обеспечение безопасности, а также рассмотрены составляющие таких этапов, включая концепцию продуктных и процессных несоответствий, применение техники IMECA и декомпозицию процесса разработки таких систем. Указаны кейсы индустриального применения предложенного подхода, а также направления дальнейших исследований.

11. РОЗРОБКА БЕЗПЕЧНОГО ПЕРСОНАЛЬНОГО КАБІНЕТУ КОРИСТУВАЧА

к.т.н., проф. Филоненко А.М., Лещенко В.О., НТУ "ХПИ", Харьков

Сьогодні сучасна людина не уявляє своє життя без інтернету і веб-сайтів. Кожен з вас реєструється в соціальних мережах, в інтернет-магазинах та на інших сайтах. Я хочу продемонструю етапи розробки сайту від вибору предметної області, створення унікального дизайну, верстки, серверного програмування та забезпечення безпеки від копіювання: фотографій, тексту та іншої інформації веб-сайту.

На сайті реалізована можливість реєстрації користувача і можливість редагування свого профілю. Головним пріоритетом є розробка персонального кабінету користувача і аналіз відвідування сайту. Вся інформація про користувача закодована спеціальними алгоритмами для забезпечення безпеки даних. Доступ до інформації з баз даних здійснюється за допомогою PHP.

Для зберігання інформації про кожного користувача використовується база даних MySQL, яка складається з таблиць, в яких зберігаються закодовані дані про користувача, які він вводив при реєстрації свого профілю на сайті.

12. РАЗРАБОТКА КОМПОНЕНТОВ СИСТЕМ АУДИТА БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ

Марченко А.О., к.т.н., доц. Узун Д.Д., НАУ им. Н.Е. Жуковского "ХАИ", Харьков

В докладе приведен сравнительный анализ наиболее распространённых инструментальных средств для проведения аудита безопасности веб-приложений. Проведен анализ сильных и слабых сторон, существующего на рынке, автоматизированного программного обеспечения для генерации отчета о результатах проведенного аудита. На основе данных, собранных с помощью Metasploit Framework, рассмотрены возможности формирования детального аудиторского отчета. В результате анализа предложено собственное программное решение для формирования отчета, при проведении аудита безопасности веб-приложений с использованием Metasploit Framework.

13. ВИДЫ АТАК НА ВЕБ САЙТЫ, ПРИЧИНЫ И СЛЕДСТВИЯ

к.т.н., проф. Гавриленко С.Ю., Кореняко И.В., НТУ "ХПИ", г. Харьков

В работе были рассмотрены следующие виды хакерских атак на веб сайты: инъекционные атаки; кроссайтовые атаки; взламывание сессии и аутентификации; переадресации UI (Clickjacking атаки); подмена кэша; атаки социального инжиниринга; кроссайтовая подделка запроса; нападение изнутри (An Insider Attack); удаленное выполнение кода атаки; DDOS атаки и способы их устранения. Показано, что конкретные атаки ведут к потерям пользователь-

ских данных в области на которую была нацелена атака. Проведено перечень технических неполадок оборудования и программного обеспечения, которые могут нанести хакерские атаки, что в конечном итоге ведет в материальному и моральному ущербу. Цель работы – выявить достоинства и недостатки современных методов защиты веб сайтов.

14. СТРУКТУРНА ОРГАНІЗАЦІЯ БАГАТОРОЗРЯДНИХ ШВИДКОДІЮЧИХ СУМАТОРІВ ПРОБЛЕМНО-ОРІЄНТОВАНИХ ПРОЦЕСОРІВ ШИФРУВАННЯ ДАНИХ

к.т.н., доц. Круліковський Б.Б., Національний університет водного господарства та природокористування, Давлетова А.Я., ТНЕУ, Тернопіль

В доповіді приведена класифікація базових компонентів проблемно-орієнтованих процесорів шифрування даних, які виконують операції додавання в якості компонентів багаторозрядних комбінаційних суматорів. Розраховані оцінки структурної, апаратної та часової складності широкого класу суматорів, у тому числі виконуючих модульні операції. Запропоновані нові структури однорозрядних та багатокаскадних суматорів, які характеризуються максимальною швидкодією на основі комбінаційних логічних схем на елементах І-НЕ. Запропоновані структури такого класу суматорів з функціями шифрування даних в якості компонентів спец процесорів шифрування даних з розрядністю 1024 біти і більше. Обгрунтована проблема застосування теоретико-числового базису Крестенсона для реалізації швидкодіючих спецпроцесорів шифрування даних.

15. ДОСЛІДЖЕННЯ ВІДКРИТИХ БАЗ ШАБЛОНІВ КІБЕРАТАК

д.т.н., с.н.с. Грищук Р.В., Охрімчук В.В., ЖВІ ім. С. П. Корольова, Житомир

У доповіді розглянуті бази шаблонів кібератак (КбА) KDD-99 та CAPEC, які сьогодні широко застосовуються на практиці. У результаті дослідження встановлено, що одним із основних недоліків бази KDD-99 є недостатня кількість шаблонів КбА типу *U2R, R2L, Probe*. Це в свою чергу, призводить до зниження ефективності використання її в локальних мережах, де ймовірність реалізації атак типу *DoS* мінімальна. Показано, що основною особливістю бази CAPEC є подання в ній опису не окремих вразливостей та критичних місць, а розкриття підходів та методик, які використовуються зловмисником для проведення КбА на КСМ. Встановлено, що основним недоліком CAPEC є відсутність у шаблонах КбА інформації про параметри мережевого з'єднання. У результаті аналізу й дослідження переваг та недоліків розглянутих вище баз доведено, що для розроблення шаблона КбА, який буде одночасно відображати як дії зловмисника, так і параметри мережевого

з'єднання, необхідно скористатися принципом комплексування баз KDD-99 та CAPEC, взявши з кожної з них їх переваги та взаємокомпенсувавши недоліки.

16. СПОСІБ ДИФЕРЕНЦІЙНОГО ЗАХИСТУ ОБ'ЄКТІВ ВІДЕОЗОБРАЖЕНЬ

д.т.н, проф. Бараннік В.В., ХУПС ім. І. Кожедуба, Харків; к.т.н, доц. Подорожняк А.О., Бондарчук В.К., НТУ "ХПІ", Харків

В доповіді розглянуто підходи до захисту статичних відеозображень. Запропоновано спосіб диференційного захисту об'єктів відеозображень, та, відповідно, метод детектування інформаційно насичених областей відеозображення, заснований на аналізі груп частотних коефіцієнтів (низькочастотних, високочастотних, загальних) дискретного косинусного перетворення. Результати використання розробленого методу показують достатню ступінь захисту відеозображень в порівняні із класичними, проте на даний момент з програшем у часі обробки.

17. ПИТАННЯ КІБЕРБЕЗПЕКИ ПРИ ВПРОВАДЖЕННІ IAAS-РІШЕНЬ ХМАРНИХ ВЕНДОРІВ

к.т.н. Ткачов В.М.,ХНУРЕ, ХНЕУ ім. С. Кузнеця, Харків; Партика С.О., ХНУРЕ, Харків

У доповіді розглянуті особливості надання послуги IaaS найбільш популярними вендорами: Google, Amazon, Microsoft. Проаналізовані найбільш вразливі місця взаємодії клієнта та вендорів на прикладі послуг від корпорації Google. Запропоновано модель процесів та критерії безпеки при наданні даного виду послуг. Проведені дослідження на прикладі запропонованої моделі щодо протидії можливим загрозам. На підставі отриманих результатів зроблені висновки щодо порушених та виявлених питань, пов'язаних із кібербезпекою при впровадженні IaaS-рішень хмарних вендорів.

18. АНАЛИЗ ПРОБЛЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В БЕСПРОВОДНЫХ СЕТЯХ НА ОСНОВЕ LTE

к.т.н. проф. Завизиступ Ю.Ю., Свиридов А.С. ХНУРЄ, Харьков

В настоящее время технология Long-Term Evolution (LTE, часто обозначается как 4G LTE – стандарт беспроводной высокоскоростной передачи данных для мобильных телефонов и других терминалов, работающих с данными) приобрела достаточную популярность и значительное распространение на большинстве континентов. Не последнюю роль в таких процессах играют ее разнообразные преимущества, включая значительно повышенный уровень безопасности. В докладе представлены результаты анализа ряда проблем, связанных с обеспечением безопасности. Так, в общем случае, можно

выделить два класса актуальных уязвимостей. Первый из них представляет собой возможность получить TMSI (Temporary Mobile Subscriber Identity – временный идентификатор мобильного телефона) – используемый в процессе установки звонка, регистрации в сети и т. д. Второй класс предусматривает проведения DDoS-атак (распределённая атака типа «отказ в обслуживании») по LTE, результатом которых при подключении к 3G или 4G, устройство принудительно подключается к менее защищенным сетям 2G. Кроме того, в докладе сформулированы возможные направления решения проблем, составляющих каждый из классов.

19. БЕЗОПАСНОСТЬ ПЕРЕДАЧИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ «ЛУКОВОЙ» МАРШРУТИЗАЦИИ

к.т.н., проф. Завизиступ Ю.Ю., Партыка С.А., Новицкий Р.В., ХНУРЄ, Харьков

В докладе представлен метод передачи информации в компьютерных сетях с использованием технологии анонимного обмена - «луковой» маршрутизации. Рассмотрены основные проблемы сетевой безопасности и вероятные пути утечки информации. Так как «луковая» маршрутизация не предоставляет гарантированную анонимность для отправителя или получателя, предложен метод решения проблемы утечки информации через анализ синхронизации. Представлена модель компьютерной сети с «луковой» маршрутизацией, учитывающей узкие места при передаче трафика. Проведенное имитационное моделирование, показало высокую эффективность предложенного метода.

20. COMPARATIVE OVERVIEW OF BASIC CYBERVULNERABILITIES OF MOBILE APPLICATIONS FOR ANDROID OPERATING SYSTEM

M.S. Dubrovskyi, S.G. Semenov NTU "KHPI", Kharkiv

With the market for mobile applications for Android platform constantly growing and more security-dependent tasks moving to mobile platforms, security of Android applications is a major concern for developers and users. In this paper, an overview of Android operating system security model is given. Components of Android application are studied, with special attention given to mechanisms of Inter-process communication via Intents. An overview of basic vulnerabilities of Android applications and vulnerabilities of IPC in Android applications is performed. Recommendations for avoiding described vulnerabilities are given.

As a result of the Android security model and IPC mechanisms overview, basic IPC vulnerabilities of Android applications are described. It is shown, that mechanism of implicit Intents is the source of the most of IPC vulnerabilities, which is connected to the inherent lack of security of the mechanism. Considering

this, it is advised to minimize usage of implicit Intents for IPC. When it is impossible to avoid using implicit Intents, source of them should be validated.

21. АНАЛИЗ ПРОБЛЕМ БЕЗОПАСНОСТИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К "УМНОМУ ДОМУ" И ИНТЕРНЕТ ВЕЩЕЙ

Здоровец Ю.В., доц. Галькевич А.А., Желтухин А.В., НАУ им. М.Е. Жуковского "ХАИ", Харьков

В связи со стремительным проникновением устройств в нашу жизнь рассматривается основные проблемы защиты сферы Интернет вещей (IoT) и «умного дома» та необходимость повышения уровня безопасности. Проанализированная трех уровневая архитектура IoT состоящая из уровня восприятия, сетевого уровня и прикладного уровня основными проблемами безопасности, которой являются: физическая безопасность приборов, угрозы целостности данных, угрозы перегрузки, перехват данных, захват узла шлюза, вирусы, обеспечение прав на интеллектуальную собственность, защита приватности и т.д. Поскольку технология IoT носить гетерогенный характер необходимо разработать и внедрить национальные стандарты и технические регламенты применения безопасности с соответствующими международными стандартами.

В работе предлагаются технические и программные автоматизированные средства обеспечения безопасности приватных данных на примере "умного дома" и IoT, которые снизят к минимуму возможность несанкционированного доступа.

22. МЕТОД ЗАХИСТУ ТЕХНОЛОГІЧНИХ ДАНИХ МОНІТОРИНГУ ОБ'ЄКТІВ НА ОСНОВІ ОБРАЗНО-КЛАСТЕРНИХ МОДЕЛЕЙ

Процюк Г. , Івано-Франківський НТУ нафти і газу, Івано-Франківськ

В доповіді викладені особливості діагностування станів екологічно-небезпечних та режимних технологічних об'єктів на основі запропонованих теоретичних положень побудови образно-кластерних моделей. Розроблена інформаційна технологія організації аналого-цифрового перетворення, кодування та цифрового опрацювання даних про технологічні стани об'єктів на основі статистичного, кореляційного, спектрального, логіко-статистичного, кластерного та ентропійного аналізу. Наведено приклад формування образно-кластерної моделі для об'єктів глибокого буріння нафтогазових свердловин на прикордонних територія та буріння на шельфі. Захист даних від несанкціонованого доступу відбувається на основі теорії стеганографії та відповідної структурної організації образно-кластерної моделі контрольованого об'єкта.

23. АРХИТЕКТУРНЫЕ АСПЕКТЫ ПРИНЦИПОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Змиевская В.Н., Анциферова О.А. НТУ "ХПИ", Харьков

Для создания эффективного аппаратно-программного обеспечения информационной безопасности (ИБ) любой системы необходимо сочетание мер следующих трех типов:

- недопущение определенных, характерных для этой системы видов нарушений ИБ;
- оперативное выявление факторов нарушений ИБ;
- реагирование на нарушения ИБ, включая ликвидацию последствий.

В докладе рассматриваются архитектурные аспекты обеспечения ИБ. В качестве одного из принципов архитектурной безопасности предлагается категорирование и разделение программ и данных. Это особенно важно при разработке и реализации программных средств обеспечения информационной безопасности, способных противостоять деструктивным воздействиям.

24. ПРОГРАММНАЯ СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

Ильина И.В. ХУ ВС им. И. Кожедуба , Харьков, Сидоренко И.И., Академия Национальной гвардии Украины, Харьков

В настоящее время актуальность эффективного управления рисками в сфере информационной безопасности трудно переоценить. В отчетах крупных компаний часто фигурируют огромные цифры финансовых потерь, понесенных в результате хакерской атаки, утраты ценных сведений и т.п.

В докладе рассмотрены современные подходы к оценке рисков неблагоприятных событий, необходимость в которых возникает при обеспечении информационной безопасности корпоративной информационной системы. Проведен анализ существующих программных систем, предназначенных для оценки таких рисков. Предложен подход к анализу рисков, основанный на построении формальных моделей прецедентов компьютерных атак. Изложены математические основы предлагаемого подхода. Описана программная реализация подхода.

25. ПРОЕКТИРОВАНИЕ И АНАЛИЗ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ НА БАЗЕ СМАРТФОНА

Елисеев Р.Ю., ХНУРЭ, Харьков

В докладе рассмотрены особенности дизайна криптографически стойких ГСЧ (ГПСЧ с источником энтропии) предназначенных для использования в первую очередь на мобильных и подобных энерго-эффективных платформах с ограниченными ресурсами. Предложена модель ГСЧ для современных те-

лефонов с источником энтропии на основе доступной устройству аудио-, видеоинформации, информации GPS/GLONASS (уровень сигнала, количество доступных спутников, координаты устройства и погрешность измерений), гироскопа/датчика положения, статистику использования батареи устройства, текущее время, информацию о телефонной книге и журнале звонков/сообщений и некоторые другие. Предложены криптопримитивы, пригодные для использования в ГСПЧ и эффективные с точки зрения производительности и потребления энергии на предложенном оборудовании. Произведен анализ статистических и криптографических свойств получаемой с помощью предложенного ГСЧ информации.

26. АНАЛІЗ МОЖЛИВИХ АТАК НА RFID МІТКИ ТА МЕТОДІВ ПРОТИДІЇ ЇМ

Левченко Д.Ю., ХНУРЕ, Харків

В доповіді розглянуті особливості використання RFID міток та ряд атак як на них(Dos – атака, яка, в цілому, є простим зашумленням робочої частоти діалогу між міткою та терміналом, RFID-Zapper, клонування вмісту пам'яті RFID – міток), так і на додатки на їх основі(переповнення буфера, SQL – ін'єкції, web – інтерфейси). Були розглянуті декілька RFID – міток відомих виробників та проаналізовано можливість здійснення атак на системи з використанням кожної з них, проведено порівняльний аналіз. Проведений аналіз показав, що незалежно від типу мітки складність здійснення атаки на додаток, що її використовує(переповнення буфера додатку), не змінюється, також існують атаки проти яких, на даний момент, не існує ефективних механізмів захисту (атака типу «man in the middle», Dos – атака). Аналіз деяких чіпів показав їх низьку стійкість до атака по побічним каналам (перехоплення інформативних сигналів під час діалогу з терміналом).

27. ОРГАНІЗАЦІЯ КОНФІДЕНЦІЙНОГО ДОКУМЕНТООБІГУ

Іващенко К.О., ХНУРЕ, Харків

У доповіді розглянуто організацію конфіденційного документообігу, метою якої є виділення інформації, що документується, та види документів, в яких вона повинна бути зафіксована. Запропонавані наступні організаційні етапи:

- встановлення всього складу циркулюючої на підприємстві інформації, а також визначення характеру додаткової інформації, що може виникнути в результаті діяльності підприємства; визначення щодо конфіденційності інформації та віднесення її до комерційної таємниці, визначення ступеня конфіденційності; визначення конкретних термінів конфіденційності конфіденційності інформації або подій, при настанні яких конфіденційність знімається.

Види конфіденційних документів необхідно встановлювати з урахуванням оптимального обсягу інформації, що міститься в них, що виключає надлишкову, у тому числі дублетну інформацію, оскільки надлишкова інформація – це конфіденційні дані, витік яких може завдати шкоди підприємству.

28. АНАЛИЗ ВОЗМОЖНЫХ АТАК НА ЭЦП И МЕТОДЫ БОРЬБЫ С НИМИ

Присяжная О.А., ХНУРЭ, Харьков

В докладе рассмотрены несколько схем построения цифровой подписи, на основе алгоритмов симметричного и асимметричного шифрования, а также их модификации, проанализированы преимущества и недостатки данных алгоритмов. Предложены преимущества, которые дает хеш-функция, а также возможные атаки на ЭЦП, которые актуальны и в настоящее время. Также в работе описана классификация возможных результатов атак. Проведенный анализ показал, что самой "опасной" является адаптивная атака на основе выбранных сообщений, и при анализе алгоритмов ЭП на криптостойкость нужно рассматривать именно её.

29. ОБЗОР БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ ICLOUD

Мирошниченко В.В., ХНУРЭ, Харьков

В докладе рассмотрены особенности хранения данных в ICLOUD, а именно шифрование данных алгоритмом AES.Также рассмотрены методы защиты информации с помощью различного новейшего программного обеспечения. Для данных ICLOUD используются "Надежные пароли", которые создаются с помощью безопасного генератора псевдослучайных чисел. Также рассмотрены дополнительные возможности повышения уровня безопасности при входе и авторизации в ICLOUD, которая заключается в инновационной двухэтапной проверке. Проведен статистический анализ взлома и хакерских атак на ICLOUD.

30. АНАЛИЗ ПОДХОДА К ПОСТРОЕНИЮ КОНЦЕПЦИИ ЗАЩИТЫ НА ОСНОВЕ ЦЕНТРАЛИЗОВАННОЙ СХЕМЫ АДМИНИСТРИРОВАНИЯ МЕХАНИЗМОВ ЗАЩИТЫ В ОС WINDOWS

Брюх Б.К., ХНУРЭ, Харьков

В статье приведен анализ выполнения ОС Windows формализованных требований к защите информации. Рассмотрен анализ подходов к построению концепции защиты на основе централизованной схемы администрирования механизмов защиты. Основной результат. Большинством современных универсальных ОС не выполняются в полном объеме требования к защите конфиденциальной информации. Это значит, что, учитывая требования нор-

мативных документов, они не могут без использования добавочных средств защиты применяться для защиты даже конфиденциальной информации. При этом следует отметить, что основные проблемы защиты здесь вызваны не невыполнимостью ОС требований к отдельным механизмам защиты, а принципиальными причинами, обусловленными реализуемой в ОС концепцией защиты. Концепция эта основана на реализации распределенной схемы администрирования механизмов защиты, что само по себе является невыполнением формализованных требований к основным механизмам защиты.

31. ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ В HTTP-ТРАФИКЕ

Цыбулька И.В., ХНУРЭ, Харьков

В работе был рассмотрен метод антивирусной защиты сервиса доступа к HTTP-ресурсам для борьбы с вредоносными программами на прокси-сервере. Предложен антивирусный ICAP-сервер, разработанный ОДО "ВирусБлокАда", обеспечивающий взаимодействие с ICAP-клиентами по протоколу ICAP версии 1.0 с возможностью осуществлять проверку в режиме preview. Был создан патч, для Squid-ICAP, для работы в режиме preview в связке со Squid-ICAP (прокси-сервер, являющийся ICAP-клиентом), обеспечивающий его стабильную работу. Предложено использовать антивирусный ICAP-сервер в режиме проверки объекта до его попадания в кеш, для повышения производительности прокси-сервера. Предложено использовать механизм, предоставляемый заголовком ISTag в протоколе ICAP, из документа RFC 3507, пункт 4.7, для обеспечения наиболее полной защиты от вредоносных программ.

32. АНАЛИЗ КОМПЛЕКСНОГО ПОДХОДА К ОБНАРУЖЕНИЮ СЕТЕВЫХ АТАК

Домонтович В. М., ХНУРЭ, Харьков

В докладе рассмотрена разработка систем обнаружения сетевых атак (СОА). Предложены специализированные программные средства, позволяющие осуществлять активный аудит и управление безопасностью (прогнозировать, обнаруживать, предупреждать, контролировать, реагировать в реальном масштабе времени на риски безопасности) в корпоративной сети. Предложена разработка методов выявления распределенных сетевых атак, использующих в комплексе современные методы поддержки принятия решений на основе теории интеллектуальных систем, позволяющих перейти при решении назад защиты продуктов и систем технологий (СИТ) от принципа "обнаружение и ликвидация" к принципу "прогнозирование и предупреждение в реальном масштабе времени". Произведен анализ подхода, объединяющий в себе метод многоагентных систем с методами адекватного выявления признаков атак на

основе статистических методов теории вероятностей, нечеткий вероятностно-статистических методов, методов теории интеллектуальных систем, а также методов искусственных нейронных сетей.

33. РЕАЛИЗАЦИЯ ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ С ИСПОЛЬЗОВАНИЕМ 32-БИТНОЙ ВЕРСИИ RSA

Кабаченко Д.О., ХНУРЭ, Харьков

В докладе описан метод реализация электронно-цифровой подписи с использованием 32-битной версии RSA. Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, предназначенный для удостоверения источника данных и защиты данного электронного документа от подделки. RSA – криптографический алгоритм с открытым ключом. RSA стал первым алгоритмом такого типа, пригодным и для шифрования и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений. Цифровая подпись обеспечивает:

- удостоверение источника документа. В зависимости от деталей определения документа могут быть подписаны такие поля, как "автор", "внесённые изменения", "метка времени" и т.д;
- защиту от изменений документа. При любом случайном или преднамеренном изменении документа (или подписи) изменится хэш, следовательно, подпись станет недействительной.

34. АНАЛИЗ МЕТОДОВ ОБУЧЕНИЯ HIPS-МОДУЛЕЙ АНТИВИРУСОВ

Новаков Е. О., Цуранов М. В. НАУ им. Н.Е.Жуковского "ХАИ", Харьков

В докладе проведен анализ основных способ построения антивирусной защиты, их преимущества и недостатки. Более подробно рассмотрены проактивные антивирусные системы. Описаны различия двух основных подходов к построению HIPS-модулей (классические и экспертные). Проведен анализ методик обучения HIPS-модулей и связанных с этим возможных проблем. Даны рекомендации по выбору подходов к обучению проактивных антивирусов. Рассмотрены различные методики обнаружения вредоносных действий в системе. Описан порядок шагов в случае обнаружения потенциально опасных для ОС операций.

35. СТРАТЕГИЯ ОБЕСПЕЧЕНИЯ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ УКРАИНЫ

Мисюра М.Ю., ХНУРЭ, Харьков

В докладе рассмотрены мероприятия по обеспечению кибербезопасности стратегия формирования государственной политики в сфере обеспечения

кибербезопасности Украины, противодействие реальным угрозам и минимизация потенциальных угроз. Обеспечение кибернитической безопасности Украины происходит с учетом положения Конституции, Закона Украины "Об основных принципах внутренней и внешней политики", Закона Украины "Об основах национальной безопасности", Стратегии национальной безопасности Украины и Доктрины информационной безопасности Украины.

Предложена система обеспечения кибернитической безопасности Украины. Предложен состав Национальной системы кибернетической безопасности. В состав Межведомственной коллегии по вопросам противодействия кибернетическим угрозам по должности входят: Премьер-министр Украины, Председатель Службы безопасности Украины, Министр внутренних дел Украины, Министр обороны Украины, начальник Генерального штаба Вооружённых сил Украины, Председатель Государственной службы специальной связи и защиты информации Украины, руководитель Государственного агентства по киберзащите.

36. АНТИВИРУСНАЯ ЗАЩИТА ПРИ НЕКОРРЕКТНО НАПИСАННОМ КОДЕ. БЕЗОПАСНОСТЬ ДАННЫХ ПРИ СКАНИРОВАНИИ АНТИВИРУСНЫМ ПО

Гамолин Р.В., ХНУРЭ, Харьков

В докладе рассмотрены различные среды виртуализации при автоматическом детектировании подозрительного ПО. Показана работа на нескольких операционных системах (ОС Microsoft Windows XP,Vista,7,8,8.1). Рассмотрены наиболее часто встречающиеся ошибки в коде программы, и влияние их на результат теста антивирусного ПО (ошибки в логической составляющей программы, неверный путь, процесс, и т.п.). Предложены варианты решения данной проблемы и модификации строк кода с ошибкой. Описан путь данных при процессе сканирования антивирусным ПО. Произведен анализ а также рассмотрены варианты утечки информации через сервер программы детектирования потенциально подозрительного ПО. Предоставлены логи ведущих программ для антивирусной защиты и обнаружения потенциально нежелательного ПО. Рассмотрен вариант взлома персонального компьютера клиента антивирусной лабораторией. Предложены пути решения данной проблемы.

37. ІНФОРМАЦІЙНА СФЕРА ТА СУСПІЛЬСТВО

Литвинчук Д.О., ХНУРЭ, Харьков

У доповіді розглянута інформаційна сфера, як системоутворюючий фактор життя суспільства, активно впливає на стан політичної, економічної, оборонної й інших складових національної безпеки України. У сучасному світі відбувається безперервна боротьба за контроль над інформаційними потока-

ми. Виграє той, хто не лише їх формує та вміє регулювати у своїх власних інтересах, але й здатний забезпечити цілісність свого інформаційного ресурсу. Розвиток наук, в першу чергу фундаментальних – математики, фізики, теорії інформації, теорії обробки сигналів та, як похідних від фундаментальних наук, радіоелектроніки, технологій виробництва радіокомпонентів, інформаційних технологій, призвели на сучасному етапі їх розвитку до виникнення інформаційного суспільства. Основою такого суспільства є інформаційні технології та інформація, яка в таких умовах стає товаром й основним продуктом виробництва та створення додаткової вартості.

38. СИСТЕМА БЕЗНАЛИЧНОЙ БЕСКОНТАКТНОЙ ОПЛАТЫ УСЛУГ ТРАНСПОРТА

Желтухин А.В., Павлюков Е.А., НАУ им. Н.Е.Жуковского «ХАИ», Харьков

В докладе рассмотрены стандарты НСМЭП. Разработана схема системы бесконтактной оплаты проезда в городском транспорте, использующая электронный кошелек. Представлена программа проверки подлинности карты, проверки и безопасного снятия суммы, соответствующей тарифу проезда. Представлен алгоритм шифрования данных для передачи по открытому каналу связи смарткарты и ридера. Рассмотрены варианты возможных угроз снятия денежных средств незарегистрированном ридером, снятии средств со сторонний карты посредством NFC и GPRS канала связи. Рассмотрены способы минимизации риска осуществления этих атак.

39. АНАЛИЗ АТАК НА SSL/TSL

Рибкін І.С., ХНУРЭ, Харьков

Огромное количество Интернет ресурсов используют реализации криптопротокола SSL/TSL, следовательно, нахождение уязвимостей является актуальной задачей. В докладе рассмотрены особенности интерфейса и известные алгоритмы атак на SSL/TSL библиотек. В ходе анализа были выявлены уязвимоти Logjam и Bar Mitzvah, и на основе проделанной работы было предложено 3 метода защиты.

40. БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ШЛЯХОМ СТВОРЕННЯ ЯКІСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Демчик С.Л., ЖВІ ім.С.П.Корольова, Житомир

У доповіді наведено шляхи вирішення проблеми щодо безпеки інформаційних систем шляхом створення якісного програмного забезпечення. Було досліджено, що найкращим способом забезпечення критеріїв конфіденційності, цілісності та доступності при розробленні та впровадженні

програм є верифікація та валідація результатів розробленого програмного продукту на кожному етапі життєвого циклу з виключенням можливості проникнення сторонніх програмних додатків всередину системи. Проведений аналіз показав, що причиною виникнення, так званих, "слабких місць", якими зловмисники користуються для атак системи, є дефекти специфікацій аналітиків та помилок проектувальників під час розроблення програмних комплексів. Внаслідок цього запропоновано механізм упорядкування плану тестування і підготовки тестів для перевірки окремих елементів розробленої програми, що призведе до збільшення ефективності захисту від збоїв апаратури і невиявлених помилок, а також правильності функціонування в заданих умовах.

41. ВДОСКОНАЛЕНІ АЛГОРИТМИ НАВЧАННЯ НЕЙРОМЕРЕЖЕВОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ БЕЗПЕЧНОГО СТАНУ НЕРУХОМИХ ОБ'ЄКТІВ СИСТЕМ КРИТИЧНОГО ЗАСТОСУВАННЯ

Конєв В.В., УДУЗТ, Харків

В доповіді доведено необхідність комплексного використання нейромережних технологій при вирішенні завдань моніторингу та ідентифікації безпечного стану нерухомих об'єктів забезпечення життєдіяльності систем критичного застосування. Розроблено відповідну структурну схему нейромережевої системи ідентифікації безпечного стану нерухомих об'єктів. Визначено необхідність вдосконалення алгоритмів навчання нейронних мереж, що входять в цілому в розроблену структуру. Запропоновано вдосконалені алгоритми навчання із застосуванням евристичної процедури для багатошарового персептрона, для радіально-базисної функції та нейронной сети Эльмана.

42. ПОСТРОЕНИЕ НЕЙРОННОЙ СЕТИ ДЛЯ РАСПОЗНАВАНИЯ МОНОХРОМНЫХ ИЗОБРАЖЕНИЙ ВОЗДУШНЫХ ОБЪЕКТОВ.

Юзова И.Ю., ХУ ВС, Харьков

Беспилотные летательные аппараты очень часто используются в качестве основного источника информации о наземной обстановке, геологической деятельности или в топографических целях. Как правило, техника позволяет получить изображения высокого качества и разрешающей способности, которые в дальнейшем передаются на пункт управления для дальнейшего анализа. На современном этапе существует большое количество методов, которые позволяют выделять отдельные объекты, устранять шумы и в разных интерпретациях так или иначе преобразовывать отдельные изображения. Существует, также, большое количество известных методов, которые позволяют распознавать объекты на исходных изображениях, огромные корпора-

ции, такие как Google и Adobe вкладывают огромное количество ресурсов для решения задачи распознавания объектов на фотографиях. Но недостатком, а точнее большим грузом является тот факт, что мировые гиганты пытаются распознать любые объекты при использовании одинакового подхода к каждому изображению. В случае, который предлагается рассмотреть, необходимо распознать именно воздушные объекты, что базируются на аэродромах. Это даёт преимущество в плане выделения характерных особенностей объектов, что распознаются. А именно, возможным становится построение стандартной нейронной сети – многослойного персептрона с 1500 нейронов на входе и 28 нейронами на выходе. В первом скрытом слое будет 15000 нейронов, во втором слое 1500, в третьем слое 150. На вход подаётся заранее преобразованное монохромное изображение трансформированное в вектор, что состоит из 0 и 1, где 0 – чёрный пиксель, а 1 – белый. Количество связей в нейронной сети будет весьма значительным (90233400), но современные вычислительные возможности обычного персонального компьютера позволяют выполнять вычисления и настройку данной нейронной сети в режиме реального времени практически без задержек. А полученная конечная реализация нейронной сети позволяет в течении миллисекунд классифицировать представленный на изображении объект.

43. ИССЛЕДОВАНИЕ МАТРИЧНЫХ МОДУЛЯРНЫХ КРИПТОСИСТЕМ

Соколов О.В., Воронин А.М., ХНУРЄ, Харьков

В данном докладе рассмотрена криптосистема BMMC, которая имеет близкий к RSA уровень безопасности к потенциальному взлому и, кроме того, в отличие от RSA, устойчива к атакам квантового компьютера. Существуют две модификации криптосистемы BMMC, а именно, MMMC1 и MMMC2, которые по теоретическим оценкам скорости шифрования существенно быстрее не только RSA, но и BMMC. Изучена обоснованность этих теоретических оценок и найдена реальная скорость шифрования компьютерных реализаций данных алгоритмов.

СЕКЦІЯ 3

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ ТА ВИКОРИСТАННЯ ЦИФРОВИХ ОБ'ЄКТІВ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Керівники секції: д.т.н., с.н.с. Семенов С.Г., НТУ "ХПІ", Харків

Секретар секції: Шипова Т.М., НТУ "ХПІ", Харків

1. ПРОБЛЕМНІ ПИТАННЯ ЗАПРОВАДЖЕННЯ ВИМОГ НОРМАТИВНО-ПРАВОВИХ АКТІВ У ГАЛУЗІ УТВОРЕННЯ, ОБРОБКИ ТА ЗНИЩЕННЯ ОКРЕМИХ ВИДІВ ІНФОРМАЦІЇ ТА ЇЇ НОСІЇВ

д.т.н., проф. Розорінов Г.М., к.т.н. Брягін О.В., ДУТ, Київ

У доповіді наведено обґрунтування введення терміну "інформація зі спеціальним процесуальним статусом" (далі - ІСПС) та надано його визначення. Основною ознакою ІСПС є обов'язкове поєднання у характеристиках інформаційного продукту науково-технічного та правового аспектів. У якості прикладу розглянуто поняття "документ" з Кримінального процесуального кодексу України. На основі аналізу положень процесуального законодавства та технологій запису інформації вперше запропоновано систематизацію ознак дуалістичної природи окремих процесуальних документів. Ознаки поділені на умовні (процесуальної змістовності, процесуальної автентичності та загальної процесуальної спроможності документу) та безумовну ознаку щодо його матеріальності. Розроблено основні вимоги до технології утворення процесуальних документів на накопичувачах Flash. Отримані результати матимуть цінність також для суб'єктів, що виготовляють та оброблюють інші види процесуальної (ліцензійної) інформації.

2. ПРАВОВЫЕ ВОПРОСЫ СТАНДАРТИЗАЦИИ ПРОЦЕССОВ ТЕСТИРОВАНИЯ ИНФОРМАЦИОННОЙ И ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ ПРОДУКТОВ РЕАЛЬНОГО ВРЕМЕНИ

д.т.н., с.н.с. Семенов С.Г., Бульба С.С., Лисица Д.А. НТУ "ХПИ", Харьков

В докладе рассматриваются правовые аспекты и основные факторы, определяющие стандартизацию процессов тестирования информационной и функциональной безопасности, надежности, а также безопасного использования программных продуктов реального времени. Анализируются характеристики таких систем и среды их функционирования, для которых должна обеспечиваться функциональная безопасность. Представлены требования к

проектным решениям, обеспечивающим функциональную пригодность сложных программ. Обсуждаются вопросы организации и планирования жизненного цикла таких программ, в том числе процессы разработки требований к их безопасности. Выделены основные международные стандарты технологических процессов, которые поддерживают функциональную безопасность в жизненном цикле сложных комплексов программ. Значительное внимание уделено испытаниям систем на функциональную безопасность используемых в их составе программных продуктов.

3. СИСТЕМА ФОРМИРОВАНИЯ ЦИФРОВОГО ИДЕНТИФИКАТОРА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЗАЩИТЫ АВТОРСКИХ ПРАВ

к.т.н. Давыдов В.В., Мовчан А.В. НТУ "ХПИ", Харьков

В соответствии со статьями 433 Гражданского кодекса Украины и 18 Закона Украины "Об авторском праве и смежных правах"– компьютерные программы (программное обеспечение) охраняются как литературные произведения. Такая охрана распространяется на компьютерные программы независимо от способа или формы их выражения.

В докладе проведен анализ проблем защиты авторских прав на программное обеспечение. Предложены пути совершенствования технических средств и механизмов защиты лицензионных прав. Разработана обобщенная структура процесса формирования цифрового идентификатора ПО. Отличительной особенностью предложенной структуры является использование формальных данными о компьютерных системах, на которые лицензионной ПО устанавливается в процессе формирования лицензионного цифрового идентификатора. Предложен алгоритм функционирования системы и генерации лицензионного ключа, адаптированный к входным данным и возможным условиям верификации ПО.

4. РЕГУЛЮВАННЯ ПОЛІТИКИ КІБЕРБЕЗПЕКИ ТА МОЖЛИВІ НАПРЯМКИ ЇЇ РОЗВИТКУ

Єрмолович А.В., ХНУРЕ, Харків

У доповіді розглянуто сучасну державну політика у сфері забезпечення кібернетичної безпеки, що має бути спрямована на забезпечення інформаційного суверенітету України у кіберпросторі, створення надійного захисту національного сегменту. Виходячи з цього розбудовувати національну систему кібербезпеки слід за трьома основними напрямами: протидія кіберзлочинності; захист вітчизняного інформаційного простору в комп'ютерних мережах; забезпечення інформаційної безпеки критичної інфраструктури. Обмеженість суто захистом державних інформаційних ресурсів не відповідає сучасним тенденціям у сфері боротьби із кіберзлочинністю. Тому актуальними як з

позиції фундаментальної теорії, так і практичної складової державного управління залишаються подальші наукові дослідження у контексті розробки дієвого механізму державного регулювання та забезпечення кібернетичної безпеки. На сьогодні реальні прояви кібератак можуть призвести до порушень функціонування інформаційно-телекомунікаційних систем, які безпосередньо впливають на стан національної безпеки і оборони. У зв'язку із цим існуючі загрози вимагають вжиття державою комплексних заходів щодо забезпечення кібербезпеки.

5. НАУЧНЫЕ ОСНОВЫ ПОЛИТИКИ КИБЕРБЕЗОПАСНОСТИ УКРАИНЫ

Дмитриев К.И., ХНУРЭ, Харьков

В докладе рассмотрены основным назначения политики кибербезопасности в обществе, которыми является сохранение самобытности наций, государств, создание реальных и действенных механизмов обеспечения информационных прав и свобод человека в киберпространстве, предотвращения манипулирования массовым сознанием. Особенности исследования научной позиции в отношении политики кибербезопасности состоят в том, что онтологически концепция политики кибербезопасности является следствием парадигмального понимания мультивекторности развития информационного общества и его многоальтернативности, невозможности заранее определить направления развития и соответственно четко урегулировать нормами права широкий спектр информационных правоотношений. Государственная политика кибербезопасности должна вытекать из требований Конституции Украины, положений Концепции государственной информационной политики, Стратегии национальной безопасности Украины.

6. КІБЕРБЕЗПЕКА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Мерцалов Д.В., ХНУРЭ, Харьков

У доповіді розглянуто сучасні механізми захисту інтелектуальної власності в глобальному інформаційному середовищі. Заохочення інноваційної діяльності та захист правовласників від кіберзагроз виходить на перший план у державних (національних) стратегіях інтелектуальної власності. Інтелектуальна власність як особливо цінний нематеріальний актив (бази даних, комерційні таємниці і ноу-хау комп'ютерних програм і т. д.) є предметом нових загроз у кіберпросторі. Кібербезпека запобігає порушенню прав інтелектуальної власності, а також забезпечує правовласникам конфіденційність баз даних, комерційної таємниці. Захист інтелектуальної власності в кіберпросторі (в тому числі сучасні технічні засоби) створює необхідний рівень конкурентоспроможності для правовласників. У першій

частині доповіді розглянуті питання впливу глобалізації інформаційного середовища, стратегії інформаційної безпеки і ІР в Україні та за кордоном з точки зору юриста. У другій частині розглянуті проблеми інтелектуальної власності в структурі кібербезпеки, комерційна таємниці та її захист від кіберзагроз. У третій частині - нові проблеми захисту доменних імен різного рівня і товарних знаків, юридичні проблеми глобалізації інтернет-торгівлі та інших послуг у мережі Інтернет.

7. НАУЧНЫЕ ОСНОВЫ ПОЛИТИКИ КИБЕРБЕЗОПАСНОСТИ УКРАИНЫ

Єрьомін А.І., ХНУРЭ, Харьков

В докладе рассмотрен глобальный рост влияния информационных технологий, безопасность этой отрасли становится главным вызовом для глобального сообщества, каждого отдельно взятого государства и человека. Новые информационно-коммуникационные технологии открывают совершенно новые возможности. Многослойные информационные потоки способствуют укреплению потенциала и нацелены на более высокий уровень развития на благо миллионов людей во всем мире. Из года в год возрастает зависимость от информационных технологий практически в любой сфере жизни, а вместе с тем, проблемы, связанные с киберпространством, приобретают всё более глобальный характер. Следовательно, государственная политика кибербезопасности должна вытекать из требований Конституции Украины, положений Концепции государственной информационной политики, Стратегии национальной безопасности Украины.

Учасники конференції

ЗМІСТ

ПЛЕНАРНЕ ЗАСІДАННЯ

СЕКЦІЯ 1
ПРОБЛЕМИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ТА ПРОГНОЗУВАННЯ ЗАГРОЗ КІБЕРБЕЗПЕКИ

СЕКЦІЯ 2
ОРГАНІЗАЦІЙНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

СЕКЦІЯ 3
ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ ТА ВИКОРИСТАННЯ ЦИФРОВИХ ОБ'ЄКТІВ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Наукове видання

ПРОБЛЕМИ НАУКОВО-ТЕХНІЧНОГО ТА ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У СУЧАСНОМУ СВІТІ

Матеріали першої міжнародної науково-практичної конференції
(30 березня – 1 квітня 2016 року)

Відповідальна за випуск *Т.М. Шипова*

Техн. редактор *Г.В. Гейко*

Коректор *С.С.Бульба*

Підписано до друку 17.03.2016 Формат 60 × 84/16
Папір офсетний Друк офсетний
Друк. арк. 3,75 Обл.-вид. арк. 3,54 Наклад 300 прим.
Ціна договірна Зам. 317-16

Адреса оргкомітету: Україна, 61002, Харків, вул. Багалія, 21, тел. (057) 707-61-65
Національний технічний університет «Харківський політехнічний інститут»

Віддруковано з готових оригінал-макетів у друкарні ФОП Петров В.В.
Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців.
Запис № 24800000000106167 від 08.01.2009.
61144, м. Харків, вул. Гв. Широнінців, 79в, к. 137, тел. (057) 778-60-34
e-mail: bookfabric@rambler.ru