НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ІНСТИТУТ КІБЕРНЕТИКИ ІМЕНІ В.М. ГЛУШКОВА
НАН УКРАЇНИ

НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ М. Є. ЖУКОВСЬКОГО

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
РАДІОЕЛЕКТРОНІКИ

НАЦІОНАЛЬНА МЕТАЛУРГІЧНА АКАДЕМІЯ УКРАЇНИ

ВІЙСЬКОВА АКАДЕМІЯ ЗБРОЙНИХ СИЛ
АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ

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

ПРОБЛЕМИ НАУКОВО-ТЕХНІЧНОГО ТА ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У СУЧАСНОМУ СВІТІ «ПНПЗК-2017»

ТЕЗИ ДОПОВІДЕЙ ДРУГОЇ МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

10 – 12 КВІТНЯ 2017 РОКУ

Харків – Київ – Дніпро – Баку – Бельсько-Бяла

2017

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова оргкомітету:

Ректор Національного технічного університету «ХПІ»,
лауреат премії НАН України імені С.О.Лебедєва,
член-кореспондент Національної академії наук України,
доктор технічних наук, професор СОКОЛ Євген Іванович

Співголови оргкомітету:

АЛІШОВ Надір Ісмаіл-Огли (д.т.н., проф., Інститут кібернетики імені В.М. Глушкова НАН України, Київ);
БАЙРАМОВ Азад Агалар-Огли (д.ф.-м.н., проф., ВА ЗС АР, Баку, Азербайджан);
КАРПІНСЬКИЙ Міколай (д.н., проф., Університет Бельсько-Бяла, Польща);
РАДЄВ Христо (д.т.н., проф., Софійський технічний університет, Болгарія);
СЕМЕНОВ Сергій Геннадійович (д.т.н., с.н.с., НТУ «ХПІ», Харків);
ШВАЧИЧ Геннадій Григорович (д.т.н., проф., НМАУ, Дніпро, Україна)

Члени оргкомітету:

АДАМЕНКО Микола Ігорович (д.т.н., проф., ХНУ, Харків, Україна);
ГАШИМОВ Ельшан Гіяс огли (к.т.н., доц., ВА ЗС АР, Баку, Азербайджан);
ДМИТРІЄНКО Валерій Дмитрович (д.т.н., проф., НТУ «ХПІ», Харків, Україна);
ЗАПОЛОВСЬКИЙ Микола Йосипович (к.т.н., проф., НТУ «ХПІ», Харків, Україна)
КОЗЛОВСЬКИЙ Валерій Валерійович (д.т.н, проф. НАУ, Київ, Україна)
КУЧУК Георгій Анатолійович (д.т.н., проф., НТУ «ХПІ», Харків, Україна);
ЛЕОНОВ Сергій Юрійович (д.т.н., доц., НТУ «ХПІ», Харків, Україна);
ЛИТВИН Василь Володимирович (д.т.н., проф., НУ "Львівська політехніка", Львів, Україна);
ЛУЖЕЦЬКИЙ Володимир Андрійович (д.т.н., проф., ВНТУ, Вінниця, Україна);
МОЖАЄВ Олександр Олександрович (д.т.н., проф., НТУ «ХПІ», Харків, Україна);
ПОВОРОЗНЮК Анатолій Іванович (д.т.н., проф., НТУ «ХПІ», Харків, Україна);
ПОРОШИН Сергій Михайлович (д.т.н., проф., НТУ «ХПІ», Харків, Україна);
РУБАН Ігор Вікторович (д.т.н., проф., ХНУРЕ, Харків, Україна);
РУДНИЦЬКИЙ Володимир Миколайович (д.т.н., проф., ЧДТУ, Черкаси, Україна);
СЕРКОВ Олександр Анатолійович (д.т.н., проф., НТУ «ХПІ», Харків, Україна);
СМІРНОВ Олексій Анатолійович (д.т.н., проф.., КНТУ, Кропивницький, Україна);
ХАЛІМОВ Геннадій Зайдулович (д.т.н., проф., ХНУРЕ, Харків, Україна).

Секретаріат оргкомітету:

БУЛЬБА Сергій Сергійович (*аспірант, НТУ «ХПІ», Харків, Україна*);
ГАВРИЛЕНКО Світлана Юріївна *(к.т.н., доц.., НТУ «ХПІ», Харків, Україна);*
ШИПОВА Тетяна Миколаївна (*аспірант, НТУ «ХПІ», Харків, Україна*);
ГОРЮШКІНА Алла Ернестівна (*асистент, НТУ «ХПІ», Харків, Україна).*

ПЛЕНАРНЕ ЗАСІДАННЯ

КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНИХ РЕСУРСІВ НА ОСНОВІ НЕРОЗКРИВНИХ ШИФРІВ

д.т.н., проф. Алішов Н.І.; Сапунова Н.О.
Інститут кібернетики імені В.М. Глушкова Національної академії наук України, Київ

Класичні концепції й алгоритми організації захисту даних від атак з боку зловмисників, як правило, ґрунтуються на криптографічних методах на основі математичних рішень, які, володіючи високим ступенем стійкості, теоретично мають уразливості, оскільки завжди є можливість розробити відповідні аналітичні методи криптоаналізу. Тому актуальним є завдання з розробки логіко-евристичних алгоритмів, які можуть бути гранично безпечними з погляду розшифрування переданих даних у комп'ютерних системах і мережах. Безумовно, ці алгоритми мають бути науково обґрунтованими. У доповіді викладено результати наукових досліджень щодо створення нерозкривних шифрів.

Як секретний ключ обирається масив істинно випадкових або псевдовипадкових чисел. Для забезпечення нерозкривності при шифруванны файлів або потокової інформації байти, що передаються, замінюються значеннями, які містяться в ключі шифрування відповідно до певної адреси-зміщення, причому ці адреси-зміщення використовуються лише один раз (правило одноразових блокнотів). На іншій стороні за прийнятими адресами-зміщеннями відновлюють байти, які відповідають байтам переданого масиву даних. Наприклад, слово «Україна», якщо перший раз передається кодом «37edf0eee3f8f9e7», то другий раз – як «eef2e0ede2f2f1», третій – як «ecf4e7f1f2e0f6» і т.д. Недолік запропонованого методу полягає в тому, що обсяг масиву ключів на основі псевдовипадкових чисел іноді в декілька разів може перевищувати обсяг переданих даних. Однак при шифруванні потокової інформації використовуються блоки ключів з певним змішенням, обсяг кожного такого блоку фактично представлений лише сотнями байтів. У доповіді докладно викладаються ці подробиці.

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

ГЕОМЕТРИЧЕСКАЯ ИНТЕРПРЕТАЦИЯ ЗАВИСИМОСТИ УРОВНЯ ПРОСТОГО РИСКА ИНФОРМАЦИОНОЙ БЕЗОПАСНОСТИ ОТ ВЕРОЯТНОСТИ ЕГО РЕАЛИЗАЦИИ

д.т.н., проф. Мохор[1] *В.В.; д.т.н., проф.* Богданов [2] *А.М,. Бакалинский*[2] *А.О., к.т.н. Цуркан*[2] *В.В.*
[1]*ИПМЭ имени Георгия Пухова НАН Украины, Киев*
[2]*ИССЗИ КПИ имени Игоря Сикорского, Киев*

В докладе рассматривается зависимость уровня простого риска информационной безопасности от вероятности его реализации и стоимости ущерба. Устанавливается нелинейный характер такой зависимости, что приводит к сложностям оценивания его величины. Упрощение этой задачи осуществляется путем ее представления в линейном виде. То есть уровень риска информационной безопасности отображается двухкомпонентной моделью на плоскости. Исходя из этого утверждения, показывается квазианалогия между представлением соотношения риск-вероятность и уравнением прямой на плоскости. Полученная прямая выходит из начала координат и располагается в первом квадранте. Устанавливаются и исследуются возможные варианты ее прохождения. Причем «идеальное соотношение» риск-вероятность получается при вероятности реализации риска ниже единицы. Это приводит к нанесению максимально возможного ущерба, то есть к уничтожению информационного актива. Благодаря такому представлению появляется возможность исследования рисков информационной безопасности с применением известных методов аналитической геометрии. Вместе с тем, представление риска в виде суммы двух и более составляющих связано с необходимостью увеличения мерности системы координат до n, что приводит к необходимости дальнейших исследований в n-мерном пространстве.

АДАПТИВНИЙ МЕТОД ВИЯВЛЕННЯ ТА ПРОТИДІЇ АТАКАМ

к.т.н. Євдокименко М.О., к.т.н., с.н.с. Єременко О.С.
Харківський національний університет радіоелектроніки, м.Харків

У докладі розглянуто особливості функціонування систем виявлення та протидії атакам IDS/IPS (Intrusion detection system/Intrusion prevention system) в телекомунікаційних мережах. Ці системи на сьогоднішній день є одним з найнеобхідніших елементів захисту будь-якої телекомунікаційної системи від різноманітних атак. Їх основне призначення – виявлення фактів несанкціонованого доступу в мережу та прийняття відповідних заходів протидії: інформування про факт вторгнення, обрив з'єднання та переналаштування брандмауера для блокування подальших дій зловмисника, тобто захист від хакерських атак і шкідливих програм. У більшості систем виявлення атак для аналізу подій, що відбулися або відбуваються в системі, використовуються два методи: пошук зловживань та виявлення аномалій. Ідея даних методів полягає в пошуку та розпізнаванні змін в системі, точніше причиною їх виникнення. У зв'язку з недоліками цих двох методів часто використовують в IDS/IPS їх комбінацію. Основним недоліком систем виявлення є складний процес адаптації до нових типів атак і нездатність аналізувати поведінку об'єктів мережі в один і той же час, на всіх рівнях. На базі виявлених недоліків існуючих IDS/IPS було запропоновано адаптивний метод виявлення та протидії атакам, який може бути покладений в основу цих систем. Приведений метод виявлення атак у телекомунікаційній мережі відрізняється від відомих введенням логічних умов для виявлення атак і математичних співвідношень, щоб максимально уникнути помилкове виявлення атак. На основі логічних правил аналізу ієрархії використовуються математичні співвідношення, які дозволяють визначити вагу факторів і оцінити їх значення в процесі прийняття рішень. Проведений аналіз показав, що запропонований адаптивний метод виявлення атак дозволяє проводити динамічний аналіз активних компонентів математичних співвідношень, парного порівняння компонентів і активних чинників протидії атакам.

ПІДВИЩЕННЯ РІВНЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ КОМП'ЮТЕРІВ ЗА ДОПОМОГОЮ АПАРАТНО-ПРОГРАМНИХ МЕРЕЖЕВИХ ЕКРАНІВ

к.т.н., проф. Скородєлов В.В., к.т.н., проф. Червонний С.Й.
Національний технічний університет «ХПІ», Харків

Захист персональних комп'ютерів (ПК) від різного виду кібератак був і залишається дуже важливою і актуальною задачею. Одним із важливих заходів захисту ПК є використання мережевих екранів (МЕ).

В останні роки ринок мережевих екранів зростав дуже швидкими темпами і результатом цього стала поява великої кількості продуктів різних фірм, які можна розділити на дві групи: програмні і апаратні МЕ. Перші, в основному, призначені для захисту ПК, а другі – для малих і середніх корпоративних мереж. Програмні МЕ дешеві, але збільшують затримки, споживають ресурси комп'ютера і не можуть захистити від вразливостей операційної системи. Апаратні МЕ дорогі і не мають недоліків програмних екранів, але складні в налаштуванні і не можуть оперувати інформацією прикладного рівня.

В роботі запропонована концепція створення апаратно-програмного мережевого екрана для персонального комп'ютера, який мав би більшість плюсів як апаратних так і програмних продуктів. Сформульовані задачі, які необхідно вирішувати при розробці такого МЕ. Проведено розподілення функцій між апаратними і програмними засобами. Розглянуті структура а також взаємодія апаратних та програмних засобів запропонованого МЕ. Приводяться результати розробки апаратних та програмних засобів такого варіанта мережевого екрана. Апаратна частина, що реалізована на потужному мікроконтролері STM 32F103 і ПЛІС EPM3064, взяла на себе ту частину функцій, яку краще виконують апаратні мережеві екрани – швидку фільтрацію мережевих пакетів. Програмна частина, яка реалізована в самому ПК, здійснює генерацію критеріїв для фільтрації і інтерфейса користувача. Причому, апаратна частина може автономно працювати навіть якщо віруси заблокували роботу програмної частини, але у цьому випадку її настройки залишаються незмінними до повернення зв'язку між апаратною і програмною частинами.

ИНТЕЛЛЕКТУАЛЬНЫЕ СРЕДСТВА АНАЛИЗА КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

д.т.н., проф. Кривуля Г.Ф., к.т.н., с.н.с. Липчанский А.И.
Харьковский национальный университет радиоэлектроники, Харьков

Для обеспечения общей кибербезопасности страны наряду с разработкой государственной стратегии необходима методика анализа угроз и оценка риска нарушения информационной безопасности существующих кибернетических систем. В докладе рассмотрено использование методов нечеткой логики для описания уровня информационных рисков. С каждым значением уровня риска связаны такие существенные параметры кибербезопасности как вероятность возникновения угрозы, а также ущерб и уязвимость как следствие угрозы. Для общей оценки информационного риска предложено использовать нечеткую переменную с пятью значениями (очень высокий, высокий, средний, низкий, очень низкий).

Очень высокий риск означает, что угроза имеет высокую вероятность появления с катастрофическими отрицательными последствиями. Необходимо незамедлительно принять меры по уменьшению риска ввиду критической уязвимости, которая ставит под сомнение возможность дальнейшей эксплуатации системы.

Высокий риск – существует значительная вероятность угрозы с отрицательным эффектом. Система находится в неустойчивом состоянии в связи с серьезной уязвимостью и ущербом.

Средний риск – имеется умеренная уязвимость, но при этом угроза может иметь серьезные негативные последствия с возможным ущербом. Уровень риска не позволяет стабильно работать.

Низкий риск означает, что угроза может иметь некоторые негативные последствия без существенного ущерба. Уровень риска позволяет работать, но имеются предпосылки к нарушению нормальной работы

Очень низкий риск означает, что угроза может иметь незначительный отрицательный эффект без ущерба. Необходимо определить, существует ли необходимость в корректирующих действиях или есть возможность принять этот риск.

СРАВНЕНИЕ ПОСТКВАНТОВЫХ КРИПТОАЛГОРИТМОВ ЦИФРОВОЙ ПОДПИСИ ПО УСЛОВНЫМ КРИТЕРИЯМ

Дубинина В.В., д.т.н проф. Потий А.В.
Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», г. Харьков

Достижения квантовых вычислений сформировали новые вызовы для классических криптографических схем. Квантовые компьютеры способны выполнять параллельные вычисления путём использования принципа суперпозиции из квантовой механики, например, n-битный квантовый регистр может одновременно находиться во всех 2n возможных состояниях.

Постквантовая криптография – это общее понятие для всех криптосистем, которые могут противостоять атакам, опирающимся на квантовые компьютеры. Постквантовая криптография изучает 4 типа криптографических алгоритмов:

– алгоритмы на основе решеток;

– мультивариативная криптография;

– преобразования на основе помехоустойчивого кодирования;

– криптография на основе хеш-преобразований.

Перспективным направлением является схема цифровых подписей на основе хеш-преобразований. Одной из таких схем является схема «Lamport and Merkle». Данная схема цифровой подписи обладает хорошими скоростными характеристиками, удобная в реализации и опирается на хорошо известный криптографический аппарат - функцию хеширования.

Важной областью применения криптографии с открытым ключом является аутентификация сообщений с помощью электронных цифровых подписей. Современные подписи имеют разные свойства и достаточно широкое применение во многих сферах, что обусловливает необходимость сравнительного анализа для разработки рекомендаций с целью дальнейшего применения выбранных крипто-примитивов.

В докладе был выполнен анализ существующих крипто-алгоритмов, представлена сравнительная характеристика между алгоритмами одного класса по условным критериям.

Анализ результатов исследования даёт основания сделать вывод о том, что с ростом длины используемых кодов, времени генерации секретных ключей, времени генерации цифровой подписи наблюдается значительный рост временных затрат на генерацию секретных ключей и наложения цифровой подписи, а время верификации подписи остается постоянным и достаточно малым.

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА ЭЛЛИПТИЧЕСКИХ КРИВЫХ ЭДВАРДСА НАД ДВОИЧНЫМ ПОЛЕМ И КАНОНИЧЕСКИХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

к.т.н. Мельникова О.А., Масленникова А.О.
Харьковский национальный университет радиоэлектроники, Харьков

Криптография эллиптических кривых на сегодняшний день является активно развивающейся областью. На эллиптических кривых основаны многие национальные и международные стандарты формирования электронной цифровой подписи, в том числе разработки перспективных проектов стандартов.

Эллиптические кривые Эдвардса являются новой нормальной формой для эллиптических кривых, обладающей свойствами, полезными при реализации криптографических систем, а также рядом преимуществ по сравнению с канонической формой Вейерштрасса. Хотя в чистом виде эллиптические кривые Эдвардса над двоичным полем незначительно проигрывают в скорости, используемые формулы легко поддаются оптимизации. В ряде работ было доказано, что производительность преобразований на эллиптических кривых Эдвардса над двоичным полем может быть увеличена таким образом, что скорость превысит скорость эквивалентной формы Вейерштрасса на 25%. Преимущество использования данных кривых в криптографии обусловлено тем, что групповой закон для них обеспечивает более высокий уровень безопасности. Например, обеспечивается высокая степень защиты от так называемой атаки стороннего канала и других специфических атак.

Другим преимуществом эллиптических кривых Эдвардса над двоичным полем является удобство реализации. В отличие от эллиптических кривых в канонической форме Вейерштрасса, эллиптические кривые Эдвардса над двоичным полем обладают свойством полноты: формула сложения «универсальна» для любых 2 точек. При реализации не возникает необходимость избыточных проверок, существенно замедляющих преобразования.

УСОВЕРШЕНСТВОВАНЫЙ МЕТОД МАСШТАБИРОВАНИЯ МЕТОДОЛОГИИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С УЧЕТОМ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ

д.т.н., проф. Рубан И.В.[1], д.т.н., с.н.с. Семенов С.Г.[2], Кассем Халифе[2]
[1] Харьковский национальный университет радиоэлектроники, Харьков
[2] Национальный технический университет «ХПИ», Харьков

В докладе рассмотрены особенности представления мультимедийного трафика гетерогенной сети в виде солитоноподобных волн. Предложена модель трафика гетерогенной компьютерной сети, основанная на его представлении в виде солитоноподобных функций, которые являются результатом решения нелинейных дифференциальных уравнений Кортевега де Вриза. Проведенный анализ показал, что данная модель точнее отображает характер наиболее нестабильных участков трафика по сравнению с существующими моделями.

Рассмотрены особенности усовершенствованного метода масштабирования методологии разработки программного обеспечения с учетом требований безопасности. Отличительные особенности метода заключаются в возможности управления существующими в организации (фирме) силами (специалистами) как в составе команды, так и в плоскости специалистов смежного направления (специалистов безопасного программирования и тестирования безопасности ПО).

Представлена математическая модель этапа инициализации процесса разработки ПО, основанная на концептуальных положениях Agile.

Так же рассмотрена математическая модель этапа реализации функционала ПО, отличающаяся от известных учетом показателей безопасного программирования.

В результате получил дальнейшее развитие способ масштабирования существующей методологии разработки с учетом требований безопасности ПО, отличающийся от известных включением и использованием в команде разработчиков дополнительных специалистов безопасности.

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ У ВИЯВЛЕННІ ВТОРГНЕНЬ

Шаповалов М.С., к.т.н., доц. Заковоротний О.Ю, ст. викл. Гугнін В.М., д.т.н., с.н.с. Семенов С.Г.
Національний технічний університет «ХПІ», Харків

В даний час в різних галузях науки і техніки підвищується інтерес до використання штучних нейронних мереж. Таку популярність нейронних мереж можна пояснити можливістю їх ефективного застосування в задачах, з якими «аналітичні» методи погано справляються. Одним із таких завдань є створення системи виявлення вторгнень.

Мінливий характер мережевих атак вимагає гнучку захисну систему, яка здатна аналізувати величезну кількість мережевого трафіку за методом, який менш структурований ніж той, що заснований на побудові певних правил. Система виявлення вторгнень на основі нейронної мережі може потенційно вирішити багато з проблем, які мають місце бути в системах, заснованих на правилах.

Реалізація нейронних мереж в системах виявлення вторгнень передбачає включення їх в існуючі або модифіковані експертні системи. На відміну від попередніх спроб використовувати нейронні мережі в виявленні аномалій, використовуючи їх в якості заміни для існуючих компонентів статистичного аналізу, цей варіант пов'язаний з використанням нейронної мережі для фільтрації вхідних даних з метою виявлення підозрілих подій, які можуть вказувати на вторгнення і направляти ці події експертної системі. Ця конфігурація поліпшить ефективність системи виявлення за рахунок зменшення помилкових тривог експертної системи. Нейронна мережа визначає ймовірність того, що певна подія є показником атаки, тому можна встановити поріг, при якому подія направляється в експертну систему для додаткового аналізу. Оскільки експертна система тільки отримує дані про події, які розглядаються як підозрілі, чутливість експертної системи може бути збільшена.

Таким чином, завдяки інтеграції нейронних мереж в систему виявлення вторгнень на основі правил, можна домогтися більшої ефективності системи в цілому та більш раціонального використання експертної системи.

АНАЛИЗ СИСТЕМ РОЛЕВОГО РАСПРЕДЕЛЕНИЯ ДОСТУПА

Лисица Д.А., Лисица А.А.
Национальный технический университет «ХПИ», Харьков

Еще одним направлением моделирования процесса распределения доступа в компьютерных системах являются модели систем ролевого распределения доступа. Анализ этих моделей показал, что ролевое распределение доступа представляет собой развитие политики дискреционного распределения доступа, при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли.

Ролевое распределение доступа является составляющей многих современных компьютерных систем. Как правило, ролевое распределение доступа применяется в системах защиты СУБД, или в элементах сетевых операционных систем.

В основе всех математических моделей данного направления лежит базовая модель ролевого распределения доступа, которая определяет самые общие принципы построения ролей.

В базовой модели ролевого распределения доступа существует ряд ограничений, позволяющих ее использовать в реальных компьютерных системах. Так, например, в базовой модели ролевого распределения доступа отсутствуют механизмы, позволяющие одной сессии активизировать другую сессию (все сессии активизируются пользователем). Еще одним важным механизмом данного направления моделирования являются ограничения, накладываемые на множества ролей, на которые может быть авторизован пользователь или на которые он авторизуется в течение одной сессии.

Одной из отличительных особенностей данного направления моделирования от других моделей стало построение системы администрирования ролевого распределения доступа. Реализация этой задачи возложена на соответствующие модели администрирования, в которых административные роли могут быть разделены на три группы по своему назначению:

– администрирование множеств авторизованных ролей пользователей;
– администрирование множеств прав доступа, которыми обладают роли;
– администрирование иерархии ролей.

АНАЛИЗ И ИССЛЕДОВАНИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ДИСКРЕЦИОННОГО РАСПРЕДЕЛЕНИЯ ДОСТУПА

Змиевская В.Н.
Национальный технический университет «ХПИ», Харьков

Проведенный анализ моделей систем дискреционного распределения доступа показали приоритетность двух направлений данного вида моделирования: матричного (модель Харрисона-Руззо-Ульмана (ХРУ), модель типизированных матриц доступа (ТМД)) и потокового (классическая модель Take-Grant, расширенная модель Take-Grant).

Основными элементами данных моделей являются множество объектов системы, множество субъектов системы, множество видов прав доступа субъектов на объекты, матрица доступов, строки которой соответствуют субъектам, а столбцы – объектам (для моделей ХРУ и ТМД), конечный помеченный ориентированный граф без петель, с множеством ребер представляющий текущие доступы к системе (для моделей Take-Grant). Решение задачи распределения доступа в данных моделях сводится к решению оптимизационной задачи на матрице или графе.

Сравнительные исследования данного направления математического моделирования позволили выявить ряд недостатков, существенно снижающих область применения моделей.

Так, например, модели ХРУ и ТМД могут выражать большое разнообразие политик дискреционного распределения доступа, но при этом не предоставляют алгоритмов проверки их безопасности. В то же время классическая и расширенная модели Take-Grant при расширении спектра политик безопасности становятся слишком громоздкими, при этом практическое их использование существенно затрудняется. Кроме этого все без исключения модели дискреционного распределения доступа статичны и не учитывают фактора внешних воздействий.

Перспективным направлением при разработке средств распределения доступа является использование интеллектуальных технологий. Это позволит компенсировать ряд недостатков существующих систем, и в комплексе использовать актуальные входные данные, как в системе обнаружения вторжений, так и в системе распределения доступа.

ОБЗОР КРИВЫХ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ

Джурик О.В.
Харьковский национальный университет радиоэлектроники, Харьков

Среди различных форм представления эллиптических кривых особое место занимает кривая в форме Эдвардса, появившаяся в современной научной литературе сравнительно недавно. Обладая рядом замечательных свойств, кривые Эдвардса над конечными полями весьма перспективны в криптографии. Закон сложения для точек кривой Эдвардса обладает свойствами универсальности и полноты. Более того, скалярное произведение для точек кривой Эдвардса вычисляется минимальным числом операций в поле по сравнению с другими известными представлениями эллиптических кривых. Несомненно, что кривые Эдвардса вызывают интерес при проектировании криптографических протоколов и будущих стандартов асимметричного шифрования

Поиск кривых Эдвардса, приемлемых для криптографии, представляет собой нетривиальную задачу. Ключевым моментом в ней является расчет порядка кривой, заданной над конечным полем. Для поиска кривых Эдвардса почти простого порядка предложен подход, в котором для найденных кривых над полями F5 и F7 с минимальным порядком 4.

На сегодняшний день открытой остается задача адаптации алгоритмов вычисления порядка кривой для кривых в форме Эдвардса. Однако приемлемые кривые Эдвардса над простыми полями можно получить посредством трансформации кривой Эдвардса в изоморфную кривую в форме Вейерштрасса с последующим определением порядка кривой в форме Вейерштрасса.

Порядок кривых, который имеет минимально возможный кофактор, равный 4, и простой кофактор, сравнимый по длине с длиной соответствующего поля делают возможным применение полученных кривых в практических приложениях.

МЕТОДИ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ

Іващенко К.О.
Харківський національний університет радіоелектроніки, м. Харків

У доповіді було розглянуто проблему нестабільного функціонування мереж передачі даних.

Метою роботи є покращення інформаційної безпеки мереж передачі даних шляхом збільшення достовірності виявлення аномалій у роботі ключових вузлів мереж передачі даних та зменшення кількості помилкових спрацьовувань при автоматизації виявлення аномалій. Аномалії визначаються як зміни показників функціонування компонентів мережі передачі даних, що свідчать про відхилення від нормального режиму роботи, зокрема про вторгнення до цих мереж. Прикладами показників функціонування може бути кількість пакетів або байтів, прийнятих або відправлених портом обладнання за одиницю часу, кількість відхилених вхідних та вихідних пакетів за одиницю часу, завантаження процесору та інше.

Під час роботи був розроблений метод побудови профілю нормального функціонування компонентів мережі передачі даних на основі адаптивної моделі тимчасового ряду, в якості якого використовується трьохпараметрична модель Уінтерса з динамічними коефіцієнтами адаптації, що забезпечує кращу реакцію моделі на зміни ряду. Також створено метод виявлення аномалій у роботі компонентів мереж передачі даних на основі динамічної оцінки відхилень фактичних значень показників функціонування від профілю нормального функціонування. Даний метод розрізняє наступні ділянки ряду: нормальний, можливого початку аномалії, аномальний, можливого завершення аномалії.

Здійснено експериментальну перевірку та оцінку ефективності розроблених методів, показано, що розроблені методи дозволяють зменшити кількість помилок першого роду (пропуск аномалії) та другого роду (помилкове спрацьовування).

АНАЛИЗ УСЛОВИЙ РЕАЛИЗАЦИИ БЕЗУСЛОВНО СТОЙКИХ ШИФРОВ

Кабаченко Д.О.
Харьковский национальный университет радиоэлектроники, Харьков

В данной работе были проанализированы условия реализации абсолютной стойких шифров на примере Шифра Вернама. Данный шифр особенно хорош тем, что для него невозможен полный перебор ключей с целью определения открытого текста по известной криптограмме. Например, при попытке перебрать все 2n возможных ключей шифра Вернама (при наличии криптограммы длиной в n бит) криптоаналитик получит вместе с истинным открытым текстом и все другие осмысленные открытые тексты той же длины. Выбрать же из них нужный открытый текст не представляется возможным. Метод шифрования, который предлагает шифр Вернама, можно было бы считать идеальным, если бы не один серьезный недостаток слишком большой расход ключевой информации. Большие трудности возникают также при попытке объединить в сети связи большое количество абонентов. Ведь в этом случае необходимо иметь возможность быстро получать доступ к любому ключу любого пользователя (которых может быть несколько тысяч). Таким образом, на практике, как правило, приходится довольствоваться шифрами, которые не являются совершенными. Данный шифр имеет множество недостатков, основной из которых – это проблема доставки ключей обоим сторонам, тем не менее, схема одноразового блокнота является единственной схемой с абсолютной стойкостью, доказанной теоретически. Вышеперечисленные недостатки можно попытаться устранить применением новых схем распределения ключей, например таких, как квантовая криптография, в частности, протокол BB84 для генерации и передачи одноразовых блокнотов. Также существуют другие перспективные методы распределения ключей, например использование возможностей нейрокриптографии.

КАЧЕСТВЕННЫЙ АНАЛИЗ И ОЦЕНКА РИСКОВ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Самсонов П.С., Спасов А.А.
Национальный технический университет «ХПИ», Харьков

В докладе представлен комплекс методов качественного анализа и количественной оценки рисков разработки программного обеспечения, что позволило решить противоречие, возникающее при разработке ПО, и заключающееся в пренебрежении фирмами-разработчиками ПО факторами 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.

Использование усовершенствованной методики «Анализа дерева отказов» позволит до 22% повысить точность количественной оценки рисков разработки ПО. В то же время использование способа оценки показателя чистой приведенной стоимости проекта разработки ПО позволяет рассматривать проект комплексно, с учетом необходимости учета безопасности и тестирование уязвимости ПО, с привлечением инструментов, которые позволяют преодолеть сложность, неопределенность и долгосрочность проектов.

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНИХ АЛГОРИТМІВ СКАЛЯРНОГО МНОЖЕННЯ В ГРУПІ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ

Біліченко Д.Г.
Харківський національний університет радіоелектроніки, Харків

У даній доповіді наведено комплексний аналіз алгоритмів скалярного множення в групі точок еліптичної кривої. Отримані результати можуть бути використані розробниками для оптимального вибору апаратних засобів в умовах обмежень по пам'яті і обчислювальних ресурсів. Отримані результати також можуть бути застосовані для прискорення роботи алгоритмів факторизації натуральних чисел і тестування чисел на простоту. Криптосистеми, засновані на еліптичних кривих, є більш ефективними щодо криптосистем першого покоління з відкритим ключем RSA і DH в разі, якщо вони будуть ґрунтуватися на швидких алгоритмах в групі точок еліптичної кривої. Докладне дослідження структури алгоритмів в групі точок еліптичної кривої дозволить отримати більш ефективні за швидкістю роботи алгоритми щодо RSA і DH при істотно більш коротких ключах. Крім того, це дозволить скоротити обчислювальну складність алгоритмів факторизації і тестування натурального числа на простоту за допомогою еліптичних кривих.

Попереднє обчислення точок широко використовується для прискорення скалярного множення в додатках, де доступна додаткова пам'ять. Відомими в цьому класі методами є метод несуміжної форми подання скаляра вікном w (wNAF) і метод зі змінним вікном(s \ wNAF). Оскільки ці методи вимагають додаткову пам'ять для зберігання попередньо обчислених точок, то пристрої з обмеженою пам'яттю не можуть задовольняти таким вимогам.

В ході проведення аналізу були вивчені чотири ефективні алгоритми обчислення скалярного множення точки і проведено порівняння їх результатів. У підсумку найбільш ефективним виявився алгоритм на основі методу несуміжної форми подання скаляра зі змінним вікном.

АНАЛІЗ МЕТОДИКИ ОЦІНКИ ЗБИТКІВ ВІД ПОРУШЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

Вітюк К.Ю.
Харківський національний університет радіоелектроніки, Харків

Збиток може проявлятись як людські, моральні або матеріальні втрати в різних сферах діяльності суб'єктів інформаційних відносин (у політичній, економічній, військовій, науково-технічної, соціальної сферах). За величиною втрат (масштабу шкоди) збитки можуть бути класифіковані як дуже значні, значні, середні, незначні і дуже незначні. Для більш детального визначення виду і величини збитку необхідно розробити (або використовувати існуючі) моделі ситуацій, що призводять до виникнення збитків у результаті порушення безпеки інформації в різних підсистемах і ланках типових об'єктів електронно-обчислювальної техніки.

У доповіді детально розглянутий приклад методики оцінки збитків від порушення інформаційної безпеки. Ця методика розподіляється на декілька етапів. Перший етап полягає у вивченні впливу загроз безпеки інформації на технічні характеристики апаратних засобів обробки інформації. На цьому ж етапі оцінюється вплив загроз безпеки інформації на якість програмних засобів і якість вхідної інформації відповідно. На другому етапі проводиться оцінка відносного зниження ефективності процесу обробки інформації, викликаного погіршенням технічних характеристик апаратних засобів, якості програмних засобів, вхідної і оброблюваної інформації. Третій етап полягає в оцінці відносного зниження ефективності розв'язуваних на об'єкті електронно-обчислювальної техніки приватних функціональних завдань, внаслідок погіршення ефективності обробки інформації. На четвертому етапі проводиться оцінка відносного зниження ефективності функціонування об'єкту електронно-обчислювальної техніки в цілому в залежності від зниження ефективності розв'язання окремих завдань на ньому. Для отримання більш наочних оцінок на кожному з етапів проводиться розрахунок втрат, пов'язаних з впливом загроз на ефективність функціонування елементів об'єкту електронно-обчислювальної техніки, процесу обробки, вирішуваних завдань.

АНАЛИЗ БИОМЕТРИЧЕСКИХ МЕТОДОВ ИДЕНТИФИКАЦИИ ПО ОТПЕЧАТКАМ ПАЛЬЦЕВ С ИСПОЛЬЗОВАНИЕМ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

Присяжная О.А.
Харьковский национальный университет радиоэлектроники, Харьков

Идентификация человека становится все более и более актуальным направлением исследований. Традиционная технология идентификации, которая использует персональнальный идентификационный номер (PIN-код), удостоверение личности или ключ, больше не считается достаточно надежной, для удовлетворения требований безопасности электронных транзакций. Все эти методы страдают от общей проблемы неспособности различать доверенное лицо и мошенника, который обманным путем получает право доступа авторизованной личности.

Биометрия является быстро развивающейся технологией, которая однозначно идентифицирует человека, основанная на его физиологических или поведенческих характеристиках.

Среди различных биометрических идентификаторов, отпечатки пальцев являются самыми старыми, наиболее используемыми. В результате анализа было выявлено, что в качестве ключевого параметра выступает вопрос о подлинности, является ли источник входного сигнала живой палец. Этот тест безопасности называется обнаружение «живучести».

В данной работе рассмотрены методы, основанные на вейвлетах, которые обнаруживают «живучести» связанные с изменениями в потовых временных сериях изображений отпечатков пальцев. Вейвлеты представляют собой математические функции, позволяющие анализировать различные частотные компоненты данных

Проведенный анализ показал, что благодаря надежности и достоверности, методы биометрической идентификации широко используются в современных информационных системах. Алгоритмы, представленные в данном докладе, являются попыткой повысить надежность системы распознавания отпечатка пальца.

АНАЛИЗ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Шипова Т.Н., Гейко Г.В.
Национальный технический университет «ХПИ», Харьков

Современные системы обнаружения вторжений (СОВ) должны обеспечивать не только пассивное блокирование несанкционированных запросов к внутренним ресурсам компьютерных систем, но и интеллектуальное перераспределение доступа к ним, с целью обеспечения ряда услуг безопасности (непрерывности функционирования, доступности информационных ресурсов и др.). Кроме того интеллектуальные СОВ должны выполнять обнаружение и регистрацию успешных сетевых атак, анализ их причин и последствий, динамическую подстройку ресурсов управления с целью устранения негативных последствий злоумышленных вторжений.

Проведенный анализ показал, что одним из самых сложных компонентов СОВ и распределения доступа является подсистема анализа (выявления нарушений безопасности), от свойств которой фактически зависит безопасность защищаемой компьютерной (телекоммуникационной) системы. Эффективность этой подсистемы в значительной степени определяется корректностью и актуальностью входных данных, возможностями используемого аппарата анализа данных о состоянии защищаемой системы, эффективностью технологий принятия решений и распределения доступа.

С целью выбора направления исследований проанализированы наиболее распространенные методы выявления нарушений информационной безопасности, определены их достоинства и недостатки. Основными недостатками являются:

- ухудшение скорости работы для журналов большого объема; необходима помощь специалистов; нет унифицированного формата хранения журналов; анализ не в реальном времени; на каждый анализируемый узел необходим свой агент,
- не чувствительны к порядку следования событий; трудность задания пороговых значений характеристик событий; «статистические» системы могут быть «обучены» нарушителями;
- повышенные требования к аппаратному обеспечению (особенно в высокоскоростных сетях); неэффективность работы в коммутируемых сетях и сетях с канальным шифрованием.

МЕТОДИ НАСКРІЗНОГО ТЕСТУВАННЯ МУЛЬТИСЕРВІСНИХ МЕРЕЖ

Можаєв О.О., Коломієць І.І.
Национальный технический университет «ХПИ», Харьков

Традиційний, проте, проблематичний підхід для отримання результатів вимірів по швидкості і надійності, з якою користувачі можуть перемикатися з каналу на канал в системах IPTV, а також отримання даних за якістю середовища передачі, фактично був побудований на основі екстенсивної тестової платформи, що складається з різних типів вимірювального лабораторного устаткування. Цей вид технології тестування, що залучає до процесу сотні реально функціонуючих STB і джерел відео сигналів разом з телефонами VoIP і персональними ПК для представлення голосового трафіку і сервісів Internet важко назвати дуже практичним і ефективним стосовно IPTV QoE. Занепокоєння передусім викликають високі капітальні витрати, необхідні для придбання тестового устаткування, його розміщення у відповідному лабораторному середовищі, а також витрати на виконання робіт інженерами і фахівцями для отримання результатів від такого роду тестів. В той час, як подібний рід суб'єктивного тестування здатний ідентифікувати поріг, при якому сервіс, що надається, не відповідає рівню очікуваної від нього якості, проте, ці тести видають дуже мало інформації про те, що ж все-таки є причиною деградації якості сервісів.

У доповіді пропонується методологія нового покоління тестування IPTV QoS, яка долає недоліки і обмеження традиційних підходів при отриманні даних від тестів за допомогою використання одиничної, уніфікованої системи тестування для симуляції і проведення тестових сесій IPTV QoE у мережевому середовищі, які точно відбивають масштаб і характеристики реально функціонуючих телекомунікаційних інфраструктур triple play. Реалістичне симуляція активності абонентів мереж triple play і що надаються цими мережами сервісів створює ідеальне середовище для оцінки рівня якості і функціонування усієї інфраструктури IPTV. Отримані результати тестування якості середовища IPTV мають бути масштабовані, повторювані і забезпечувати можливість «глибинного погляду» на причини, що стоять за збоями у функціонуванні.

МОДЕЛЬ НАРУШИТЕЛЯ ПРАВ ДОСТУПА В АВТОМАТИЗИРОВАННОЙ БАНКОВСКОЙ СИСТЕМЕ НА ОСНОВЕ СИНЕРГЕТИЧЕСКОГО ПОДХОДА

к.т.н., с.н.с. Евсеев С. П., к.т.н., доц. Король О.Г.
Харьковский национальный экономический университет им. С. Кузнеца, Харьков

Впервые предложенная в работе модель нарушителя прав доступа в АБС (Автоматизированная Банковская Система) разработана на основе методологии и синергетическом подходе к обеспечению безопасности БИн. Она позволяет систематизировать классификацию нарушителей и обеспечить построение перечня актуальных угроз для каждой категории нарушителей. При исключении субъектов атак из числа потенциальных нарушителей можно уменьшить максимальную категорию нарушителя, а, следовательно, и количество актуальных угроз. Данная модель отличается оригинальной однозначной классификацией нарушителей прав доступа в АБС в соответствии с уровнями их воздействия на АБС, обеспечить возбуждение в системе обеспечения банковской информации управляемых эмерджентных свойств, направленных на получение синергетического эффекта, который достигается благодаря качественно новому подходу к обеспечению безопасности.

Предложенный модифицированный классификатор угроз в АБС ОБС обеспечивает связь модели нарушителя с моделью угроз, позволяет сформировать соответствующие метрики угроз и превентивных защитных мер, семантику и систему кодирования различных классов угроз в АБС ОБС. Применение предложенной модели нарушителя и классификатора угроз позволяет избежать привлечения специалистов по защите информации на этапе предпроектного обследования.

АНАЛИЗ МЕТОДОВ СЖАТИЯ ДАННЫХ ДЛЯ СТЕГАНОГРАФИЧЕСКИХ ЦЕЛЕЙ

Литвиненко О.Е.
Национальный технический университет «ХПИ», Харьков

В докладе проведен анализ основных методов сжатия данных. Определено, что все алгоритмы сжатия оперируют входным потоком информации, минимальной единицей которой является бит, а максимальной – несколько бит, байт или несколько байт. Целью процесса сжатия, как правило, есть получение более компактного выходного потока информационных единиц из некоторого изначально некомпактного входного потока при помощи некоторого их преобразования. Основными техническими характеристиками процессов сжатия и результатов их работы являются:

- степень сжатия (compress rating) или отношение (ratio) объемов исходного и результирующего потоков;
- скорость сжатия - время, затрачиваемое на сжатие некоторого объема информации входного потока, до получения из него эквивалентного выходного потока;
- качество сжатия - величина, показывающая на сколько сильно упакован выходной поток, при помощи применения к нему повторного сжатия по этому же или иному алгоритму.

По критерию, связанному с характером или форматом данных, все способы сжатия можно разделить на две категории: обратимое и необратимое сжатие.

Проведенные исследования показали, что для реализации стеганографических функций целесообразно использовать методы необратимого сжатия данных.

РАЗРАБОТКА СИСТЕМЫ ПРИНЯТИЯ РЕШЕНИЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Челак В.В., к.т.н., проф. Гавриленко С.Ю.
Национальный технический университет «ХПИ», Харьков

В докладе представлена система принятия решений (СПР), для обнаружения вредоносного программного обеспечения на основе вероятностного автомата.

СПР регулирует значения таблицы вероятностей переходов автомата и управляет функционированием автомата.

Текущая вероятность $P_{ij}\ (X,\ t)$ определяется следующим образом (1):

$$\mathrm{P_{ij}}\left(\mathrm{X,t}\right)=\left\{\begin{array}{c}0,\mathrm{S_{ij}^{A}}\left(\mathrm{X}\right)=\mathrm{S_{z}^{A}}\\ \mathrm{P_{ij}}\left(\mathrm{X,t-1}\right),\mathrm{S_{ij}^{A}}\left(\mathrm{X}\right)\neq\mathrm{S_{z}^{A}}\wedge\mathrm{S_{ij}^{H}}\left(\mathrm{X}\right)=\mathrm{S_{z}^{H}}\\ \mathrm{P_{ij}}\left(\mathrm{X,t-1}\right)+\mathrm{M},\mathrm{S_{ij}^{H}}\left(\mathrm{X}\right)\neq\mathrm{S_{z}^{H}}\end{array}\right\} \quad (1)$$

где $P_{ij}\left(X,t\right)$ – рассчитываемое значение вероятности переходов в таблице для *i*-го столбца и *j*-ой строки, $P_{ij}\left(X,t-1\right)$ – текущее значение таблицы вероятности, S_z^A все элементы множества состояний-предков, исключая текущий элемент, $\mathrm{S_{ij}^{A}}\left(\mathrm{X}\right)$ – элемент из множества предков, которому соответствует вероятность P_{ij} , S_z^H - множество наследников, включает все элементы кроме текущего ($S_{ij}^H\left(X\right)$), *M* – маркерное значение (принимает значения -1 до 1).

Полученные результаты тестирования предложенной системы, подтвердили возможность ее использования, как средства выявления вирусных атак в общей системе обнаружения вредоносного программного обеспечения.

СЕКЦІЯ 2

ОРГАНІЗАЦІЙНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ.

Керівники секції: д.т.н., проф. Кучук Г.А., НТУ «ХПІ», Харків

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

ЗАХИСТ ІНФОРМАЦІЇ В СУЧАСНИХ СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ

к.т.н., доц. Миронець І.В., Бардаков Я.А.
Черкаський державний технологічний університет, Черкаси

Мобільний зв'язок – це електрозв'язок, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися в межах усіх пунктів телекомунікаційної мережі, зберігаючи єдиний унікальний ідентифікаційний номер мобільної станції. Проблема захисту інформації в таких системах є досить актуальною, оскільки в наш час не можна уявити життя без мобільного зв'язку. В таких системах передавання інформації між мобільною й базовою станціями відбувається радіоканалом, що накладає досить жорсткі вимоги на забезпечення їхньої інформаційної безпеки, яка реалізується на основі відповідних криптографічних алгоритмів. Стандарти мобільного зв'язку умовно поділяють на три покоління мереж: 1G - аналоговий мобільний зв'язок, де передавання даних не передбачено; 2G - цифровий мобільний зв'язок, в яких голос передається вже в цифровому вигляді та з'являється можливість передавати цифрові дані; 3G - широкосмуговий цифровий мобільний зв'язок, комутований багатоцільовими комп'ютерними мережами. Даний зв'язок дає можливість здійснювати відеодзвінки, широкосмуговий доступ в Інтернет, а також переглядати потокове відео в online. У стільникових стандартах третього покоління (3G) використовуються більш криптостійкі протоколи забезпечення безпеки системи, що включають використання 128-бітного секретного і аутентифікаційного ключів. Технологічні рішення і стійкі криптографічні протоколи, що знайшли застосування в цьому стандарті, забезпечують високий рівень конфіденційності мереж, побудованих на його основі. Протоколи, що забезпечують безпеку передавання інформації в CDMA-IS-41 мережах, є одними з кращих в індустрії. Крім того сам CDMA стандарт за своєю побудовою робить перехоплення сигналу, розшифрування якого є дуже складним завданням, що потребує значних фінансових вкладень.

АЛГОРИТМ АНАЛИЗА УЯЗВИМОСТИ SQL INJECTION ДЛЯ УПРАВЛЕНИЯ РИСКАМИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

д.т.н., проф. Смирнов А.А., к.т.н., доц. Коваленко А.В., к.т.н. Коваленко А.С.
Центральноукраинский национальный технический университет, м. Кропивницкий

В докладе рассмотрена SQL инъекция, которая возможна, если входные данные используются в запросах к БД без предварительной валидации. В данной реализации выполняется анализ параметров GET запроса на предмет наличия уязвимости:

1) Из переданной приложению URL веб-приложения извлекаются параметры GET-запроса и добавляются в список подлежащих проверке.

Например, для ссылки http://www.mysite.com/mypage.html?var1=value1&var2=value2&var3=value3 таким списком будет следующий – [var1, var2, var3].

2) Выполняется слепая (blind) SQL инъекция. Данный подвид атаки заключается в том, что через уязвимый параметр передаются два запроса – один с выражением, которое всегда истинно (Пример: /?id=10 AND 1=1), и второй – с выражением, которое всегда ложно (Пример: /?id=10 AND 1=0). Формируется тестовая ссылка, куда подставляется инъекция, например

http://www.mysite.com/mypage.html?var1=value1 AND 1=1 и осуществляется переход по ссылке. Затем, формируется ссылка

http://www.mysite.com/mypage.html?var1=value1 AND 1=0 и осуществляется переход по ссылке. В случае, если результаты выполнения запроса будут отличаться, можно говорить о наличии уязвимости к SQL инъекциям.

3) Выполняется SQL инъекция с объединением запросов. В этом случае, выполняется объединение значения параметра с другим запросом с помощью операции UNION языка SQL.

(Пример: http://www.mysite.com/mypage.html?var1=value1 UNION SELECT * FROM USERS)

После чего осуществляется переход по ссылке и получение ответа от сервера. Если в ответе сервера будет результат объединенного запроса либо текст ошибки базы данных, по которому можно идентифицировать базу данных, можно говорить о наличии уязвимости к SQL инъекциям.

4) Шаги 2 и 3 повторяются для каждого элемента списка параметров GET запроса.

БЕЗПЕКА У ANDROID

д.т.н., проф. Кучук Г.А., Гугнін В.М., Межерицький С.Г.,
Мельников О.С.
Національний технічний університет «ХПІ», Харків

Найбільшу долю операційних систем на ринку смартфонів займає Android (станом на 2016 року – 86.2%), що покладає на Google відповідальність за безпеку даних всіх користувачів.

Нещодавно професор криптографії Метью Грін з університету Джона Хопкінса стверджував, що Android відстає в плані безпеки від iOS як мінімум на шість років.

При цьому директор з безпеки Android Адріан Людвіг нещодавно заявив, що число Android-смартфонів, на яких встановлено потенційно небезпечні програми, становить менше 1%.

Побачивши ці заяви ми вирішили дізнатися більше про безпеку Android та дослідити розвиток та нововведення.

У докладі розглянуто особливості безпеки ядра Android, яке побудовано на базі ядра Linux.

Безпека ядра Linux заснована на користувальницькій моделі повноважень, ізоляції процесів, механізмі для безпечного IPC та можливості видалення непотрібних та потенційно небезпечних частин ядра.

Android має середовище стилю UNIX, що гарантує, що один користувач не може змінити файли іншого користувача, тобто кожен застосунок, яких вже на 2015 рік було 1,6 мільйонів, працює як власний користувач файлової системи.

Android забезпечує ряд криптографічних API, що включають реалізацію стандарту і зазвичай використовують криптографічні примітиви, такі як AES, RSA, DSA і SHA.

Крім того, API забезпечено для високорівневих протоколів, таких як SSL і HTTPS.

У останній версії Android 7.0 було введено десятки змін, деякі з яких – це засноване на файлі шифрування, рандомизація порядку завантаження бібліотеки і схема v2 підпису APK.

Розглянуті параметри безпеки та її нововведення у системі Android демонструють, що компанія Google піклується за безпеку користувачів та займає гідний рівень серед систем на ринку.

MACHINE LEARNING AND ITS APPLICATIONS IN INFORMATION SECURITY

Shnepov Aleksey, Ph.D. prof. Semenov Sergey
Kharkiv National University of Radioelectronics (KNURE), Kharkiv

Machine learning systems are systems which can increase their own quality after using some amount of data. This process is called "model learning" and usually happens on a special training set of data before systems goes live. Such systems are very popular last years and have very big success in different kinds of areas. Many of them even do their work better than human. Basically, it happens to tasks for which human usually spends less than one second or more than several years.

There are three types of machine learning: supervised learning; unsupervised learning; reinforcement learning.

First one is much more popular than others. Its name means that learning is performed on a set of input data and output data. So a destination of such learning is finding of a function which maps input to output. So as we can see this type of machine learning is designed to solve a task which is very similar to cryptanalysis one. Since cryptanalysis, also searches functions which map, for example ciphertext to plain one.

And it was already demonstrated in a series of works. The best results which I managed to find is breaking DES and Triple DES algorithms what required even less pairs of ciphertext/plaintest than it needs for liner attacks. So it looks very nice and much more results can be achieved in this area.

Also traditional machine learning application is image recognition. And it is very danger for CAPTCHAs which are used on many sites. Since for now it is not a big deal to recognise CAPTCHAs which are usually used and a creation of more complex ones leads to situations when they will be not recognisable even for humans. So this is why Google developed their "reCAPTCHA" which is a free service that protects websites from spam and abuse. It uses an advanced risk analysis engine and adaptive CAPTCHAs to keep automated software from engaging in abusive activities. It does this while letting valid users pass through with ease.

And in the end machine learning systems are used to filter emails and protect users from spam in messages. Big corporations such Google use their own systems which are very complex and distributed. Basically, these systems use some king of ratings for words, hosts, domains and so on. But actually it is not very hard to implement some own simple and in the same time effective filter using machine learning. An example of such filter is Naive Bayes classifier and its modifications.

ПРОБЛЕМИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНОЇ СИСТЕМИ RSA

к.т.н. доц. Пєвнєв В.Я., Передерій Т.С.
Національний аерокосмічний університет ім. Н.Є. Жуковського «ХАІ», м. Харків

Сьогодні людство стикається з проблемою передачі все більших і більших обсягів інформації. Актуальною на даний час є проблема захисту інформації від несанкціонованого доступу. Найбільш ефективним криптографічним засобом захисту інформації є алгоритм шифрування RSA.

Сучасні криптографічні системи з відкритим ключем будуються на базі великого простого числа. Криптографічна система RSA потребує вибору простих чисел, від яких визначається якість шифрування. Великі прості числа можна вибирати порівняно швидко. При цьому можна забезпечити їх випадковий розподіл в заданому діапазоні. Найбільш ефективним засобом вибору простих чисел є модифікована мала теорема Ферма. Однак, цей метод не дозволяє перевіряти великі прості числа. Використання ймовірнісних методів щодо таких чисел також займає дуже великий час.

Захист криптосистеми RSA побудований на факторизації великих чисел. Факторизація 512-бітного модуля реальною є вже сьогодні. Не потрібно відкривати нові алгоритми факторизації, немає необхідності в збільшенні числа комп'ютерів або в більш продуктивних комп'ютерах - досить знайти потрібну кількість учасників і скористатися вільним часом їх робочих станцій. Наприклад, лише комп'ютери компанії Silicon Graphics можуть факторизувати 512-бітний модуль за півроку при умові, що будуть вільними дві третини робочого часу.

Можливість гарантованої оцінки захищеності алгоритму RSA використовується в банківських комп'ютерних мережах, особливо для роботи з віддаленими клієнтами (обслуговування кредитних карток,тощо).

На даний час не достатньо вирішені проблеми: практичної (генерація великих простих чисел) та обчислювальної реалізації(використання довгої арифметики),а також ключі якої довжини слід використовувати.

У доповіді проведено аналіз існуючих визначень псевдо прості чисел, дано теоретично обґрунтоване визначення псевдо простого числа, розглянуто підхід до побудови великих простих чисел, який використовує псевдо прості числа. Використання таких чисел дозволяє скоротити час находження простого числа в декілька разів. Надано схема експерименту побудови псевдо простих чисел розміру 416D. Результати проведеного експерименту підтверджують теоретичні висновки о швидкодії запропонованого методу.

СИСТЕМА ШИФРУВАННЯ ВІДЕОІНФОРМАЦІЇ НА ОСНОВІ КЛІТИННИХ АВТОМАТІВ

Демаш А.А., к.т.н., доц. Білан С.М.
Державний науково-дослідний інститут спеціального зв'язку та захисту інформації України, м. Київ

У доповіді розглядаються підходи та основні проблеми існуючих методів шифрування відеоінформації. Описаний метод шифрування відеоданих на основі клітинних автоматів, який дозволяє підвищити надійність захисту відеоінформації, збільшити довжину ключа шифрування, підвищити швидкодію засекречування зображення та спростити підготовку початкових установок блоку формування підключів. Описана програмно-апаратна реалізація генератора підключів для системи шифрування відеоінформації, в основу якої покладено вищезазначений метод. Даний генератор реалізований з використанням двох клітинних автоматів, що дозволяє формувати ключову гаму у неявному вигляді. Основний клітинний автомат здійснює передачу сигналу збудження від клітини до клітини, а додатковий клітинний автомат здійснює зміну станів усіх власних клітин згідно заданої функції та вибраної околиці. Гама залежить від початкової карти станів клітинних автоматів та початкових налаштувань траєкторії руху. Генератор реалізований на дешевих ПЛІС з високими показниками по швидкодії, що дозволяє зашифровувати відеоінформацію в реальному часі в процесі передачі її по каналах зв'язку

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ПРИ ОБМЕНЕ ФАЙЛАМИ ЧЕРЕЗ НЕЗАЩИЩЕННУЮ СРЕДУ

Елисеев Р.Ю.
Харьковский национальный университет радиоэлектроники, Харьков

В докладе рассмотрены основные подходы и методы обеспечения конфиденциальности и (опционально) целостности данных при их передаче через незащищенные гетерогенные среды. End-to-end шифрование рассмотрено в призме национальной системы сертификации средств технической защиты информации. Рассмотрены базовые требования и необходимые документы для успешного прохождения государственной экспертизы комплексных средств защиты информации в интеллектуально-телекоммуникационных системах для использования в государственных органах и организациях или частных организациях, обрабатывающих данные, принадлежащие государству.

Предложена простая универсальная система шифрованной синхронизации файлов через сторонние незащищенные или слабо защищенные серверы обмена открытыми данными (файлообменники, публичные FTP серверы, сервисы синхронизации файлов Яндекс.Диск и Google Drive).

Рассмотрена возможность выполнения синхронизации каталогов удаленных систем в автоматическом режиме с сохранением конфиденциальности и опциональной целостности через популярные средства связи: email, ряд современных и устаревших IM-мессенджеров (Skype, Jabber, ICQ, Viber), социальные сети и устаревшие средства связи, как, например, IRC каналы, SMS/MMS.

Представлен краткий обзор существующих на сегодняшний день криптографических библиотек с действующими позитивными экспертными заключениеми и возможности их применения в потенциальных проектах. Обоснована необходимость разработки криптографических библиотек, соответствующих критериям прохождения государственной экспертизы, с открытым исходным кодом или бесплатных кроссплатформенных решений, включающих современные криптографические алгоритмы и подходы к их реализации.

МОЖЛИВОСТІ СУЧАСНОГО ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЕННЯ

Єрмолович А.В.
Харківський національний університет радіоелектроніки, Харків

Сучасні комп'ютерні системи є вразливими. Атаки здійснюються за допомогою спеціально розробленого програмного забезпечення, що використовує вразливості комп'ютерних систем. Все шкідливе програмне забезпечення прийнято класифікувати на класичні комп'ютерні віруси (virus), мережеві черв'яки (worms), "троянські коні" (trojan), спеціальні засоби (експлойти, генератори ключів тощо).

Існує 5 основних типів trojan: віддалений доступ, знищення даних, завантажувач, сервер, дезактиватор програм безпеки. Троян, його основною метою яких є шкідливий вплив по відношенню до комп'ютерної системи. Трояни відрізняються відсутністю механізму створення власних копій. Деякі трояни здатні до автономного подолання систем захисту комп'ютерної системи з метою проникнення та зараження системи. У загальному випадку, троян потрапляє в систему разом з вірусом або хробаком, в результаті необачних дій користувача або ж активних дій зловмисників. Також існують програми або окремі функції програм, які приховано впроваджують у комп'ютерну систему, тривалого часу функціонують у системі, порушуючи політику безпеки. Програмні закладки можуть впроваджуватись вірусом, троянським конем, черв'яком або безпосередньо користувачем-зловмисником. Функції: перехоплення і передавання інформації (Spyware), порушення функціонування систем ("логічні бомби"), утиліти віддаленого адміністрування (люки, backdoor). Це дозволяє проводити несанкціоновану роботу з мережею: інтернет-клікери, проксі-серевера; організація DoS і DdoS атак; проксі-сервера. Руткіти (rootkit) – програмні закладки або їхні компоненти, призначені для приховування слідів присутності зловмисника чи зловмисної програми у системі. Наприклад, у 2010 році було виявлено шкідливе програмне забезпечення Stuxnet, яке продемонструвало реальність загроз, які до того вважали лише уявними: програма була здатна атакувати локальні мережі, не підключені до Інтернету; призначена для атаки на промислове обладнання ядерного об'єкта.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ С ПОМОЩЬЮ ТЕХНОЛОГИИ FPGA

Колесник И.Н., к.т.н., доц. Куланов В.А.
Национальный аэрокосмический университет «ХАИ», Харьков

В настоящее время не существует универсальных готовых решений для полноценной защиты облачных сервисов от атак в силу их большого разнообразия. Исследуя разные уровни информационной безопасности между потребителем услуг и облачным провайдером, становится очевидным, что для создания надежной системы защиты облачной инфраструктуры необходимо учитывать ее конкретную архитектурную реализацию. При этом, безопасность облачных вычислений является одним из основных требований пользователей. Именно поэтому новые подходы и технологии в области защиты информации настолько актуальны и востребованы, ведь они решают самую насущную задачу – сделать облачные вычисления более безопасными.

Наблюдается тенденция к поиску и применению специализированных решений, способных многократно превзойти традиционные архитектурные методы построения высокопроизводительных серверов и вычислителей, предназначенных для решения задач защиты информации. Одним из таких решений является использование программируемой логики. С помощью микросхемы ПЛИС класса FPGA, можно уменьшить риски на предотвращение множества сценариев атак. Кроме того, важной особенностью FPGA как компонента систем обеспечения безопасности является возможность перепрограммирования. Любое обновление или изменение требований к безопасности может быть быстро реализовано в FPGA без необходимости физического изменения оборудования. Изменения и обновления требований могут быть загружены непосредственно на оборудовании и обновляется по мере необходимости.

M2M TECHNOLOGY. POTENTIAL SECURITY ISSUES

Voronkin Ivan, Ph.D. prof. Semenov Sergey
Kharkiv National University of Radioelectronics (KNURE), Kharkiv

Machine-to-Machine (M2M) communications, also called MTC for Machine-Type-Communication refer to communications between small and inexpensive devices where no or little human intervention is required.

This technology is constantly evolving and covering more and more applications. The applications currently proposed can be classified according to their field of application into five categories, namely Automotive, eHealth, Smart metering, City Automation and last but not least Home Automation.

As they rely on the fusion of heterogeneous networks, M2M communications have to cope with all the security threats of other network-based communications. Even though M2M have not induced new threats, they have amplified the existing ones as, in the case of M2M, these threats lead to not only financial losses but also pose a threat to human lives.

We can identify some of the main threats against M2M communications while classifying them into three categories depending on the targeted entities, i.e. the M2M device itself, the proper functioning of the system or the exchanged data. Accordingly - physical, logical and attack data.

Physical attacks aim to the physical layer as well as M2M devices hardware and software. Often main vector of attack it's software modification and malwares or physical Destruction or theft of the M2M device.

Logical attacks are targeting the proper functioning of the system without making any changes to the device's software. For example: Denial of Service (DoS), M2M-spoofing.

Data attacks are targeting the exchanged information. First of all there are "privacy attacks", data modification and false information injection or selective forwarding/interception.

The specific nature of M2M networks generally comprising thousands of devices, makes securing them a challenging task. But main problem is not Scalability. Most M2M devices suffer from resource constraints (energy, storage and computing), that's why the key challenge is analyze M2M applications characteristics and requirements and found proper security solutions which will satisfy main security requirements without resource overspending.

Thus, M2M system exposed to the same security threats as well as other communication systems, however, the sensitivity of the information processed, making these attacks more damaging. That's why the protection M2M is becoming urgent and requires special attention.

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ В КРИПТОГРАФІЇ

Коломоєць Р.С., д.т.н., проф. Дмитрієнко В.Д.
Національний технічний університет «ХПІ», Харків

Штучні нейронні мережі завдяки своїй архітектурі являють собою ефективний спосіб паралельної обробки даних. Дана властивість нейронних мереж дозволяє в перспективі застосовувати їх для широкого кола задач, проте часто складність реалізації такої системи заважає практичній реалізації даних систем. Але не дивлячись на цей факт штучні нейронні мережі достатньо широко використовуються для захисту інформації, як в рамках науково-дослідних проектів, так і в рамках комерційних продуктів.

Існують рішення, які дозволяють забезпечувати доступність даних. Системи цифрових водяних знаків, які побудовані з використанням нейронних мереж, дозволяють забезпечувати захист авторського права та ін.

Побудова функції хешування з використанням штучних нейронних мереж. Дослідження показують, що алгоритм хешування з використанням нейронних мереж має властивість однобічності, високої чутливості вихідного значення к вхідним даним і ключу користувача. Також даний алгоритм захищений від ряду атак. Модель нейронної мережі дозволяє всі розрахунки проводити паралельно, що прискорює роботу алгоритму.

Шифрування. Також модель нейронної мережі підходить для задач шифрування. Нейронні мережі використовуються для класифікації та апроксимації функцій задач, для яких є багато доступних даних для навчання, але до яких не можуть бути застосовані жорсткі правила. Такий алгоритм шифрування захищений до деяких атак, які застосовуються на відомі алгоритми шифрування, але в той же час такий алгоритм є складнішим в реалізації.

ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ВЕБ-ПРИЛОЖЕНИЯХ

Кочетов В. А.
Национальный технический университет «ХПИ», Харьков

На сегодняшний день интернет предоставляет огромное количество разнообразных по своей структуре инструментов для общения. Однако, начиная использовать подобные средства, пользователь оставляет часть своих персональных данных, которыми может являться только реальное имя, а могут быть и адрес проживания, или номер мобильного телефона. Для предотвращения подобной утечки информации, постоянно разрабатываются более совершенные механизмы защиты, чем существующие в данный момент.

В статье были рассмотрены способы защиты информации, предоставляемые в популярных высокоуровневых языках программирования серверной части (поскольку именно сервером обрабатывается вся информация о пользователе). Рассмотрен способ хеширования паролей с помощью bcrypt – адаптивной криптографической функции формирования ключа на основе таблицы salt, а также его более современный потомок scrypt – криптографическая функция формирования ключа на основе пароля; представлены сравнительные характеристики по сравнению с иными средствами хеширования на которых явно можно увидеть, что данные способы являются наиболее современными и надежными, но и требуют соответствующей вычислительной мощности. Также, в статье описаны общие методы для защиты, непривязанные к каким-либо условиям разработки. Примером послужил протокол взаимодействия с web-сервером https, который гарантирует безопасную передачу информации в сети.

Программной защиты часто бывает недостаточно, поскольку пользователь сам может предоставить злоумышленникам персональные данные и не подозревать об этом. С такой проблемой сталкивается, фактически, каждый интернет ресурс, и, дабы не потерять пользователя, техническая поддержка интернет портала обязуется вернуть пользователю его аккаунт и хранимые на нем, персональные данные, разумеется, если пользователь сможет подтвердить право владения аккаунтом. Нельзя оставить без внимания письма с подтверждением регистрации или входа после неоднократного неправильного ввода данных для аутентификации. Подобная схема приобрела новый цвет в современной разработке, поскольку былые письма переросли в sms, отправляемые web-приложением на телефон пользователя, что имеет меньший шанс перехвата злоумышленниками.

НАПРЯМЛЕНІ ТА ЛАЗЕРНІ МІКРОФОНИ, МЕТОДИ ЗАХИСТУ ВІД НИХ

Курбатов О. С.
Харківський національний університет радіоелектроніки, Харків

У доповіді приводяться основні пристрої для розвідки інформації з обмеженим доступом, що може витікати вібро-акустичними полями.

При організації прослуховування розмов у приміщенні, доступ до якого неможливий, можна використовувати напрямлені мікрофони та лазерні акустичні локаційні системи.

На практиці використовуються три види напрямлених мікрофонів: параболічні (рефлекторні), трубчаті («мікрофон – труба») та плоскі фазовані решітки.

Параболічний мікрофон представляє собою відбивач звука параболічної форми з високочутливим мікрофоном посередині. Параболічний відбивач може бути виготовлений як з оптично прозорого, так і з оптично непрозорого матеріалу (наприклад лист алюмінію). Принцип роботи параболічного мікрофону наступні: звукові хвилі відбиваючись від параболічного відбивача сумуються у точці фокусу, де розташований високочутливий мікрофон, тим самим збільшуючи акустичне поле. Чим більший діаметр параболічного відбивача, тим більше посилення може забезпечити мікрофон. Параболічний мікрофон є яскравим прикладом високочутливого, але слабонапрямленого мікрофону.

У плоских фазованих решітках виникає одночасний прийом звукового сигналу у різних точках площини, які знаходяться перпендикулярно до джерела звуку. В цих точках розташовують або мікрофони, або відкриті трубки – звуководи. В суматорі такого мікрофону сигнали з осьового напрямку приходять у фазі, що викликає підсилення основного сигналу. Так же як і у мікрофонів параболоїдного типу рівень сигналу буде значно зменшуватися при відхиленні від осі. Важливою перевагою фазованих решіток є можливість їх прихованого використання для сбору інформації, забезпечена відносно невеликими розмірами такого мікрофону.

Принцип роботи трубчастих мікрофонів відрізняється тим, що посилюється сигнал, який приходить вздовж певної лінії, а не перпендикулярно до площини зйому. Такий тип мікрофону складається з жорсткої трубки діаметром від 1 до 3 см, зі спеціальними отворами, які забезпечують відсіювання звукових хвиль, які приходять с неосьового напрямку. За рахунок однакової швидкості акустичних хвиль як в трубці, так і поза нею, виникає підсилення сигналу в трубці зовнішнім сигналом через отвори в трубці. Якість результуючого сигналу напряму залежить від довжини трубки.

Лазерний мікрофон для акустичного спостереження представляє собою пристрій для збору інформації на далеких відстанях, в якому використовується інфрачервоний лазерний промінь, саме за допомогою якого здійснюється підслуховування розмов цільового об'єкту. Він складається з трьох основних елементів: лазерного передатчика, лазерного приймача та блоку підсилення з записуючим пристроєм. Лазерний мікрофон детектує вібрації віконного скла, які визиваються звуковими хвилями усередині кімнати, та передає їх на приймач. Лазерний промінь, відбиваючись від віконного скла перетворюється у форму електричних сигналів, після чого проводиться фільтрація і підсилення сигналів та запис їх на виділений блок пам'яті, який підключений до власного підсилювача оснащеного гучномовцем. Таким чином моніторинг сигналу можна проводити в режимі реального часу та після запису.

Захист мовної інформації від витоку її вібро-акустичними каналами може здійснюватися завдяки зниженню відношення сигнал – шум на границях контрольованої зони. Методи захисту включають в себе пасивні – фільтрацію та послаблення вібраціонних коливань та активні – збільшення рівня перешкоджаючих сигналів з допомогою генераторів шуму.

До методів захисту мовної інформації від прослуховування її з допомогою лазерних мікрофонів також відносяться пасивні та активні методи захисту. До пасивних відносяться: зміна властивостей відбиваючої поверхності – використання матового скла, потрійні склопакети; використання менш схильних до вібрації матеріалів – наприклад пластик значно гірше передає вібрацію сигналів, ніж скло; використання приміщень, вікна яких виходять до контрольованої зони. До активних відносять системи акустичного зашумлення та системи вібраціонного захисту.

DOS И DDOS АТАКИ

Наумов А.Н.
Харьковский национальный университет радиоэлектроники, Харьков

В современном мире, где ключевую роль играет информация, не менее важной является информационная безопасность. Существует много желающих получить доступ к чужой информации или же как-то повлиять на неё. Одним из таких методов являются DoS (DDoS) атаки.

DoS-атака (атака типа «отказ в обслуживании», от англ. Denial of Service) – атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ затруднён. Отказ «вражеской» системы может быть и шагом к овладению системой (если в нештатной ситуации ПО выдаёт какую-либо критическую информацию – например, версию, часть программного кода и т. д.). Но чаще это мера экономического давления: простои службы, приносящей доход, счета от провайдера и меры по уходу от атаки ощутимо бьют «цель» по карману.

Если атака выполняется одновременно с большого числа компьютеров, говорят о DDoS-атаке (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). В некоторых случаях к фактической DDoS-атаке приводит непреднамеренное действие, например, размещение на популярном интернет-ресурсе ссылки на сайт, размещённый на не очень производительном сервере (слэшдот-эффект). Большой наплыв пользователей приводит к превышению допустимой нагрузки на сервер и, следовательно, отказу в обслуживании части из них.

DoS (DDoS) атака не нова, однако всё так же популярна и широко используемая. Во избежание проблем, которые могут возникнуть после атак данного типа, необходимо знать как их избежать.

IP-СПУФИНГ КАК ВИД СЕТЕВЫХ АТАК

Нечволод К.В.
Харьковский национальный университет радиоэлектроники, Харьков

В современном мире информационные технологии используются практически во всех сферах человеческой жизни. Большой интерес для злоумышленников представляют сетевые технологии, так как можно совершать преступления «не выходя из дома». Существует множество видов сетевых атак и одной из наиболее интересных является IP-спуфинг.

IP-спуфинг происходит, когда злоумышленник, находящийся внутри корпорации или вне ее выдает себя за санкционированного пользователя. Это можно сделать двумя способами. Во-первых, злоумышленник может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример – атака DoS, которая начинается с чужого адреса, скрывающего истинную личность злоумышленника. Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами. Для двусторонней связи злоумышленник должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Некоторые злоумышленники, однако, даже не пытаются получить ответ от приложений. Если главная задача состоит в получении от системы важного файла, ответы приложений не имеют значения. Если же злоумышленнику удается поменять таблицы маршрутизации и направить трафик на ложный IP-адрес, злоумышленник получит все пакеты и сможет отвечать на них так, будто он является санкционированным пользователем.

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Нікішин Д.Г.
Харьковский национальный университет радиоэлектроники, Харьков

Сьогодні основною цінністю для суспільства поступово стають інформаційні ресурси (ІР), які мають велику роль практично в усіх сферах життєдіяльності нашої держави. На основі вчасно наданої, достовірної і повної інформації приймаються управлінські рішення. Тому перед державою стоїть важливе завдання – удосконалення процесу використання ІР та розробка дієвих методик забезпечення захисту інформаційних ресурсів. Під інформаційним ресурсом, як правило, розуміють власне інформацію або будь-який об'єкт, що є елементом певної інформаційної технології.

Щоб забезпечити захист ІР розглянемо які існують для них джерела загроз:

– персонал (людина);
– технічні пристрої;
– програми;
– технологічні схеми обробки;
– зовнішнє середовище.

Загрози інформаційним ресурсів може бути здійснено:

– методами, які використовують психологічні особливості людей;
– шляхом підкупу осіб, які безпосередньо працюють на підприємстві або структурах,безпосередньо пов'язаних з його діяльністю;
– шляхом перехоплення інформації, що циркулює в засобах і системах зв'язку таобчислювальної техніки;
– шляхом підслуховування конфіденційних переговорів.

Існують такі методи захисту ІР:

1) Інженерно-технічний метод, який забезпечує захист інформації від витоку технічними каналами.

2) Правові та організаційні методи, що створюють нормативну базу для організаціїрізного роду діяльності, пов'язаної з забезпеченням інформаційної безпеки.

Для вирішення багатьох проблем забезпечення інформаційної безпеки необхідно застосування відповідних заходів, до числа яких належать: законодавчі, організаційні і програмно-технічні.

АНАЛИЗ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ХРАНИЛИЩ ДАННЫХ ОТ DDoS АТАК

Семашко Э.С.
Харьковский национальный университет радиоэлектроники, Харьков

Цель DDoS-атаки – заблокировать на некоторое время доступ к онлайн-ресурсу путем перегрузки канала «мусорными» запросами, в результате чего бизнес несет существенные финансовые и репутационные потери. Ситуация усугубляется тем, что DDoS-атаку сегодня может организовать практически любой желающий – стоимость ее невелика, контакты исполнителей можно найти при помощи поисковых сервисов. Такая доступность и простота организации DDoS-атаки ставят под угрозу практически любую компанию, у которой есть недоброжелатели.

В докладе рассматриваются механизмы защиты от DDoS-атак на основе облачного хранения данных.

Облачные хранилища решают задачу защищиты от DDoS-атак, если реализуются следующие требования:

- распределенность – наличие нескольких географически разнесенных узлов, чтобы вывод из строя любого из них не оказывал влияния на сервис облака.
- собственная автономная система и собственные адресные блоки, из которых для защищаемого сервиса выделяется новый IP-адрес, скрывающий истинное его расположение в сети.
- глобальная связность автономной системы с Интернетом; провайдеры облачных сервисов обеспечат клиентам, находящимся под защитой облачного решения, услугу, того что их трафик не будет теряться вне зависимости от видов атак.
- полная автоматизация процесса фильтрации.
- постоянная фильтрация должна быть приоритетной услугой, и включать протоколы BGP и DNS и реализовывать их переключение.
- использование технологии MPLS (Multiprotocol Label Switching) VPN в качестве резервной связности системы защиты и сервера.
- использование статического контента на CDN.

Вывод. Лучшей практикой защиты DDoS-атак является использование облачных решений. Эффективным методом защиты является анализ и мониторинг трафика с использованием снифферов в службах HTTP.

АНАЛИЗ МЕТОДОВ СЖАТИЯ ДАННЫХ

Сума Абубакар, д.т.н., с.н.с. Семенов С.Г.
Национальный технический университет «ХПИ», г. Харьков

В настоящее время стремительное развитие баз данных (БД) порождает необходимость хранения и обработки все больших объемов информации, что требует огромных вычислительных и временных затрат. Для сокращения объемов БД и ускорения выдачи необходимой информации по запросу, целесообразно применять методы сжатия информации.

В докладе представлены результаты анализа методов сжатия данных. Определено, что для определения методов и алгоритмов сжатия, наиболее эффективных при обработке различных типов данных целесообразно произвести их упорядочение и выбор критериев сопоставления их характеристик. В области сжатия данных действует закон противостояния, когда алгоритмы, использующие больше ресурсов (времени и памяти), обычно достигают лучшей степени сжатия, и наоборот, менее ресурсоемкие алгоритмы по качеству сжатия, как правило, уступают более ресурсоемким. Таким образом, построение оптимального с практической точки зрения алгоритма сжатия данных представляется сложной задачей, так как необходимо добиться достаточно высокого качества сжатия при небольшом объеме используемых ресурсов.

Литература 1. Семенов С.Г. Методи обробки сигналів, даних та зображень / С.Г. Семенов, О.О. Кузнецов, Г.А. Кучук – Х.: НТУ «ХПИ» 2011р. 301 с. 2. Смірнов О.А. Методи та засоби обробки сигналів і даних в інформаційних системах / О.А. Смірнов, Є.В. Мелешко, С.Г. Семенов – Кіровоград, Харків 2012р. 252 с. 3. Сжатие данных [Электронный ресурс]. – Режим доступа : http://ru.wikipedia.org/wiki/Сжатие данных.

ТЕСТУВАННЯ ТА СТВОРЕННЯ МЕРЕЖЕВИХ ІГР В NET ТЕХНОЛОГІЇ

к.т.н., проф. Лобода Є.О., Мошкін А.С.
Національний технічний університет «ХПИ», м. Харків

Розповсюдження комп'ютерів для прискорення науково-технічного прогресу викликало багато проблем для користувачів та розробників програмного забезпечення. Несумісність – сама гостра проблема сучасної індустрії програмування. Нелегко інтегрувати модулі, написані на різних мовах програмування. Програми, що виповнюються на різних машинах, для взаємообміну даними повинні перебороти величезні труднощі. Рішенням цих і багатьох інших проблем є технологія .NET, яка використовується у даному проекті.

В даний час відсутні загальнодоступні, прості в експлуатації пакети тестування швидкодії графіки мережених ігор, які засновані на порівнянні класичної і .NET технологій. Тому даний проект присвячений створенню такого пакета (оболонки) з діалоговим вікном простим в експлуатації, що працює в найбільш розповсюдженому операційному середовищі Windows із встановленим пакетом .NET Framework.

Для тестування графіки створюються дві оболонки тестування. Перша – з використанням класичної технології компіляції, друга – з використанням сучасної технології .NET. Оболонка тестування інтегрована у додаток виведення графіки. Тестується час виведення графічного образу без руху. Робиться три виміри часу: два до та один після виведення графіки. Для більшої точності тестування, проводимо вимір для кожних 1000 циклів виведення. Зі ста вимірів обирається найменший, щоб зробити мінімальним вплив допоміжних програм Windows на тестування. Після тестування за класичною технологією результати записуються у файл звіту. Аналогічно проводиться тестування за .NET технологією з записом результати у другий файл звіту тестування. Для перегляду відповідних результатів тестування використовується як .NET, так і класична оболонка.

Систему тестування з діалоговим вікном інтерфейсу користувача, отримує від користувача назву потрібного оболонці типу програми (сервер або клієнт), можливість зміни параметрів настройки зображення та звуку гри, змінювати зовнішній вигляд діалогового вікна. Тестування швидкодії виведення графіки, зберігає результати тестування у додатковому файлі і виводиться раніше отриманих результатів тестування.

Об'єкт розробки – діалогова оболонка отримання на дисплеї комп'ютера мережевої гри. Мета проектування програми - синтез мережевої гри і зміна її характеристик, тестування швидкодії виведення графіки з можливістю збереження результатів тестування. Розроблено алгоритми вирішення поставленого завдання і виконаний дизайн інтерфейсу з користувачем. В результаті цього істотно спрощена інтерфейс користувача.

СИСТЕМА АНАЛІЗУ ПОТОЧНОГО СТАНУ АДРЕСНОГО ПРОСТОРУ RAM

к.т.н., проф. Лобода Є.О., Хрипко Д.О.
Національний технічний університет «ХПІ», м. Харкі.

Сучасні завдання для програмування потребують, звичайно, великих обсягів оперативної пам'яті, інколи, перевищуючих розмір реальної оперативної пам'яті використовуваних комп'ютерів. Велика потреба в експлуатації програм вирішення проблем такого напрямку й відсутність простих їх реалізацій робить підвищений інтерес до проектів такого напрямку.

На жаль, ретельний пошук можливих діючих рішень для цього завдання показав: до сих пір відсутнє самостійне програмне забезпечення, яке дозволяє отримувати таку інформацію.

Зараз відомі ряд програм тестування пам'яті комп'ютерів. Практично всі вони аналізують тільки фізичну пам'ять. Тонкощі спілкування з віртуальною пам'яттю - не розглядається.

Для усунення цього недоліку в даному проекті реалізується діалогове вікно, що дозволяє користувачеві в простій (зрозумілій) формі для будь-якої частини віртуальної пам'яті комп'ютера створювати додатково регіон – область пам'яті, необхідну для виконання чергового фрагменту алгоритму тестування. Для цього використаються відповідні API-функції. Після закінчення виконання цього фрагмента алгоритму тестування виконується повернення простору регіону в загальні ресурси додатка (системи).

Мета проекту – розробка й програмна реалізація системи тестування працездатності віртуальної пам'яті використовуваного комп'ютера. Реалізований діалоговий режим користувача дозволяє виконувати: резервування регіонів, виділення для них фізичної пам'яті, запис у них інформації, зміну атрибутів захисту пам'яті, блокування й очищення фізичної й віртуальної пам'яті. Реалізація цих технологій роботи з віртуальною й фізичною пам'яттю комп'ютера істотно підвищує швидкість обміну й пошуку інформації в системах з великими інформаційними базами. Зміни у віртуальній пам'яті відображаються графічно у побудованому діалоговому вікні.

При виділенні фізичної пам'яті, можна задати її сторінкам до 8 типів різних атрибутів захисту, що обмежують різним способом несанкціонований доступ і/або розв'язне спільне використання декільком процесам. Переваги описаної технології роботи з пам'яттю дають явний виграш у порівнянні з: класичним оголошенням масиву, тому що, скорочуються витрати фізичної пам'яті.

Крім цього є можливість спостерігати за локальним станом введення в одному потоці та коректно повідомлти інформацію про вікнах зроблені іншими потоками.

ОБОЛОНКА РОБОТИ З ФРАКТАЛАМИ

к.т.н., проф. Лобода Є.О., студент Т. Гаурав
Національний технічний унівеситет «ХПІ», м. Харків

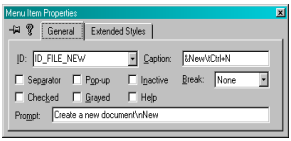
У практичній діяльності багатьох виробничих підприємств різних галузей господарства досить часто потрібно синтезувати і широко використовувати різні, важко піддаються словесному і / або математичному опису графічні зображення. Наприклад, малюнок на черговій партії тканини для швейної промисловості.

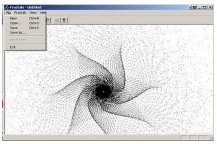
Для отримання чергового, оригінального, неповторюваного малюнка професіонали-дизайнери використовують, досить часто, фрактальні малюнки. Фрактальний малюнок – результат отримання рішення досить простої у виконанні математичної формули. Простота обчислень формул фракталів є основною перевагою отримання графічних зображень на комп'ютері. Відомо, що швидкість отримання складних графічних зображень формулами фракталів набагато вище формування стандартними функціями графічних примітивів графічних бібліотек.

В даний час відсутні загальнодоступні, прості в експлуатації пакети отримання фрактальних кривих. Тому даний проект присвячений створенню такого пакета (оболонки) з діалоговим вікном простим в експлуатації, що працюють під будь-якою версією найбільш поширеного операційного середовища – Windows.

Було прийнято рішення розробити діалогову оболонку отримання фрактальних зображень, яка отримує від користувача ім'я бажаного типу фрактального зображення, можливість автоматичної зміни параметрів фрактала, змінювати зовнішній вигляд діалогового вікна, зберігати зображення в файлі і виводити раніше створені файли фрак талів. Зараз найбільш розповсюджено використання формул фракталов – множини Мандельброта. Але оболонка дозволяє використовувати й інші формули, та створювати свої варіанти формул побудови фракталів. Крітеріем створення нових формул є те, що найважливішою особливістю всіх множин фракталів є їх само подібність – нескінченне повторення одного і того ж фрагмента зображення, але в різних масштабах.

Нижче наведено зменшені приклади зображень меню завдання параметрів чергового фрактала і оболонки з намальованим на її вікні зображенням фрактала





ТЕСТУВАННЯ БИСТРОДІЇ ГРАФІЧНИХ РЕЖИМІВ В NET ТЕХНОЛОГІЇ

к.т.н., проф. Лобода Є.О., Ю.В. Мірошник
Національний технічний університет «ХПІ», м. Харків

Розповсюдження комп'ютерів потрібне для розвитку усіх напрямків діяльності суспільства, але це викликало і багато проблем для користувачів та розробників програмного забезпечення. Несумісність – сама гостра проблема сучасної індустрії програмування. Програми, що виповнюються на різних машинах, для обміну даними повинні перебороти величезні труднощі. Додатки для різних операційних систем написані із застосуванням несумісних API (application programming interface), що ускладнює перенесення.

Рішенням цих і багатьох інших проблем є технологія .NET, яка використовується у даному проекті.

В даний час відсутні загальнодоступні, прості в експлуатації пакети тестування швидкодії графіки, які засновані на порівнянні класичної і .NET технологій. Тому даний проект присвячений створенню такого простого пакета, що працює в найбільш розповсюдженому операційному середовищі Windows із встановленим пакетом .NET Framework.

Звісно, що основною, найбільш швидкодіючою є графічна бібліотека DirectX. Складається вона з набору компонентів, що підтримують безпосередню роботу з пристроями, і служить як засіб розробки швидкодіючих мультимедійних додатків. Для програміста застосування DirectX полягає у використанні набору низькорівневих інтерфейсів API (Application Programming Interface).

Основною частиною DirectX є його частина – 'Direct3D, тому що/вона забезпечує найбільш високу швидкодію графіки постійним застосовуванням апаратного прискорення – акселераторів графічних адаптерів, що прискорюють виконання виводу зображень у сотні – тлячи разів.

Для функціонування проекту була створена велика бібліотека класів та ряд ресурсів. Всі з цих ресурсів є текстурами.

Оболонка тестування графіки була протестована на різних останніх версіях WINDOWS, але різниця між операційними системами була незначною, тому результати приведені тільки для Windows 10, з використанням різних типів графічних адаптерів. Було створено дві оболонки: за .NET технологією (speed_test_net.exe) та за класичною технологією (speed_test.exe).

Тестування проводилось з використанням мікропроцесора AMD Athlon та встановленої оперативної пам'яті 256Мб для двох типів графічних адаптерів: 1. nVidia GeForce MX 440 (64 Мб); 2. nVidia GeForce FX5200 (128 Мб)

Тестування підтвердило головну роль акселераторів у прискорені виводу.

ПРОБЛЕМИ ІНТЕРАКТИВНОГО ОБМІНУ ІНФОРМАЦІЄЮ У РОЗПОДІЛЬНОМУ ГРАЛЬНОМУ СЕРЕДОВИЩІ

Орлов Д.М., Бреславець В.С.
Національний технічний університет «ХПІ», м. Харків

Чим більше інтерактивні мобільні додатки, тим складніше стає обмін даними між мобільними пристроями і хмарної інфраструктурою. Якщо додати фактор відмінностей в швидкості передачі даних у операторів зв'язку по всьому світу - отримуємо систему, в якій для забезпечення необхідної користувачам швидкості потрібно враховувати безліч параметрів. Важливим фактором, що впливає на продуктивність додатку та передачі даних до хмарних сервісів в різних регіонах, становлять відмінності між мобільними операторами в різних частинах світу. Таким чином, щоб гра могла працювати в мобільних пристроях з низькою пропускною здатністю виникають проблеми, які більше стосуються маркетингових програм операторів зв'язку. Але несправності можуть виникати і з боку хмарної інфраструктури. У теорії, хмарні сервіси обробки інформації мають справлятися з періодами пікових навантажень, спрощуючи управління додатком, а послуги, що надаються постачальниками хмарних рішень, повинні спростити розробку різних мобільних додатків (не тільки ігор). І можливості хмар дійсно спростили використання нових можливостей, які потребують великих обчислювальних потужностей (таких як доповнена реальність). Успіх додатку підвищує навантаження на платформу провиною чому можуть стати перевантажені сервери. Розробляючи продукт потрібно прораховувати масштаби використання, щоб не виправляти безліч помилок, одночасно вирішуючи проблеми з серверними потужностями. Але, враховуючи досвід у випадках з іншими мережевими платформами минулого, зрозуміло, що наявність всіх цих потужностей не має значення, якщо відсутня можливість підключення до них.

МИКРОПРОЦЕССОРНЫЙ ГЕНЕРАТОР ПАРОЛЕЙ НА МИКРОКОНТРОЛЛЕРЕ PIC16F877A

Токарев М.Г., к.т.н., доц. Подорожняк А.А.
Национальный технический университет «ХПИ», Харьков

Современная информатика широко использует псевдослучайные числа в самых разных приложениях – от метода Монте-Карло и имитационного моделирования до криптографии. При этом от качества используемых псевдослучайных последовательностей чисел (ПСЧ) напрямую зависит качество получаемых результатов.

В докладе рассмотрены принципы генерации ПСЧ, генерация псевдослучайный последовательностей с помощью хеш-функций и применение ПСЧ и хеш функций для генераторов паролей. Важность выбора надежного источника энтропии и его влияние на распределенность генерируемых последовательностей и следовательно паролей. Рассмотрены сильные и слабые стороны некоторых популярных существующих решений (C random, xxHash).

Предложен оригинальный алгоритм генерации паролей с использованием интервалов нажатия клавиш в качестве надежного источника энтропии. Представлены результаты исследования известных и предложенного алгоритма. Проведенный анализ показал, что данный алгоритм позволяет генерировать значительно более надежные пароли чем существующие на данный момент решения.

Было разработано устройство, позволяющее генерировать 16-значные пароли несколькими способами, в том числе и с использованием датчика температуры и предложенного метода генерации. Проведено моделирование его работы в системе Proteus и тестирование на микропроцессорном стенде PIC EASY.

Целью дальнейших исследований является повышение надежности полученных результатов и уменьшение времени генерации пролей.

СНИФЕР ПАКЕТОВ – ОДИН ИЗ ОСНОВНЫХ СЕТЕВЫХ АТАК

Танянский А.Ю.
Харьковский национальный университет радиоэлектроники, Харьков

«Сетевые атаки» – сегодня это словосочетание знакомо любому пользователю компьютера. Многие уже успели стать жертвами злоумышленников. Говоря об угрозах в информационной сфере, мы не можем избежать хотя бы краткого описания типов сетевых атак. Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Одной из таких атак является сниффер пакетов.

Сниффер пакетов представляет собой прикладную программу, которая использует сетевую карту, работающую в режиме promiscuous mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки). При этом сниффер перехватывает все сетевые пакеты, которые передаются через определенный домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (telnet, FTP, SMTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли). Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам.

Важно понять, что сетевая безопасность - это эволюционный процесс. Нет ни одного продукта, способного предоставить корпорации «полную безопасность».

МЕТОДИ ПРОТИДІЇ АТАКАМ ВЕРТИКАЛЬНОЇ ЕСКАЛАЦІЇ ПРИВІЛЕГІЙ WINDOWS СИСТЕМ

Левченко Д.Ю.
Харківський національний університет радіоелектроніки, м.Харків

У доповіді розглянуті особливості реалізації атаки «ескалація превілегій», що характеризується використанням методів соціальної інженерії та вразливостей операційних систем сімейства Windows та розповсюдженого програмного забезпечення, що працює в системі. Даний тип підвищення привілегій описує ситуацію, коли користувач має або може отримати вищий рівень доступу, ніж йому належить мати за допомогою спеціалізованого програмного забезпечення та навичок роботи, адміністрування систем Windows. Проведений аналіз методології реалізації атаки даного виду показав, що 45% успішно реалізованих загроз були проведені за допомогою методів соціальної інженерії. В ході роботи були запропоновані основні методи протидії даного виду аткам як організаційними, так і технічними методами.

Основними заходами для протидії атакам такого виду є встановлення чіткої політики розмежування доступу користувачів у локальній обчислювальній мережі; регулярне тестування системи на проникнення; контроль за виходом користувачів до незахищеного середовища через власні пристрої, що під'єднані до бездротової мережі організації; обмеження доступу користувачів до інтернету; справність та правильне налаштування адміністратором безпеки міжмережевого екрану, фаєрволу та проксі серверу; встановлення заборони на використання стороннього або не ліцензованого програмного забезпечення (за допомогою встановлення політики безпеки, що забороняє запуск та інсталяцію програмних продуктів, які не входять в список дозволених) та технічних засобів (заборона автоматичної істаляції будь-яких драйверів).

В роботі запропоновано розробку методики виявлення наявності проведення та ліквідації наслідків атаки ескалації привілегій.

Розглянуто основні ризики щодо реалізації даної атаки методом соціальної інженерії та шляхом інсайдерських дій. Наведено перелік чинників, що спонукають співробітників організації до дій що призводять до компрометації системи, шляхом надання доступу та деталей побудови та налаштувань системи.

IP-СПУФИНГ

Матвиенко А.С.
Харьковский национальный университет радиоэлектроники, Харьков

IP-спуфинг происходит, когда хакер, находящийся внутри корпорации или вне ее выдает себя за санкционированного пользователя. Это можно сделать двумя способами. Во-первых, хакер может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример – атака DoS, которая начинается с чужого адреса, скрывающего истинную личность хакера.

Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами. Для двусторонней связи хакер должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Некоторые хакеры, однако, даже не пытаются получить ответ от приложений. Если главная задача состоит в получении от системы важного файла, ответы приложений не имеют значения.

Если же хакеру удается поменять таблицы маршрутизации и направить трафик на ложный IP-адрес, хакер получит все пакеты и сможет отвечать на них так, будто он является санкционированным пользователем.

Угрозу спуфинга можно ослабить (но не устранить). Наиболее эффективный метод борьбы с IP-спуфингом тот же, что и в случае со сниффингом пакетов: необходимо сделать атаку абсолютно неэффективной. IP-спуфинг может функционировать только при условии, что аутентификация происходит на базе IP-адресов. Поэтому внедрение дополнительных методов аутентификации делает этот вид атак бесполезными. Лучшим видом дополнительной аутентификации является криптографическая. Если она невозможна, хорошие результаты может дать двухфакторная аутентификация с использованием одноразовых паролей.

МЕТОДИКА СОЗДАНИЯ АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА БАЗЕ МНОГОУРОВНЕГО АНАЛИЗА КАРТ ОПЕРАЦИОННОЙ СИСТЕМЫ

к.т.н., доц. Гавриленко С.Ю., Шевердин И. В.
Национальный технический университет «ХПИ», Харьков

В докладе предложена разработка многоуровневой антивирусной системы формирования карт (MAP – Monitor Automatic Page), базирующаяся на поведенческом анализе процессов в операционной системе. Анализ процессов позволяет обнаружить все виды вирусных атак, так как для выполнения какого-либо вредоносного воздействия вирусу необходим процесс. Даже если данный вирус является набором скриптов, будут использованы интерпретаторы операционной системы, которые в свою очередь так же являются процессами.

Архитектурно, данная система является операционно- зависимой, что позволяет обеспечит формирование карт для конкретно выполняемой гостевой операционной системы, основываясь на различии драйверов устройств и различных системных компонентов.

Для построения карточного анализа используется многоуровневая система анализа поведения состояний операционной системы. Основной принцип работы данной системы, это формирование карт уровней 0 и 1 и выполнение их анализа на основе методов нечеткой логики.

Список литературы: 1. The best antivirus protection of 2017. [Электронный ресурс] – Режим доступу: http://uk.pcmag.com/antivirus-reviews/8141/guide/the-best-antivirus-protection-of-2017. 2. B. Kosko, “Fuzzy cognitive maps” *Int. Journal of Man–Machine Studies*, vol. 24, pp. 65–75, 1986 3. Decision theory [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Decision_theory 4. Decision theory [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Fuzzy_logic.

АНАЛИЗ КОМПОНЕНТОВ СИСТЕМЫ ЗАЩИТЫ ОТ КИБЕРАТАК ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ ФИТНЕС ПРИЛОЖЕНИЙ

Велигоша А.А., Цуранов М.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», г. Харьков

Все больше людей для мониторинга своей физической активности прибегают к использованию специальных фитнес приложений, однако никто не задумывается, как киберпреступники могут использовать эти данные и насколько актуальна их защита. Прежде всего имеются в виду данные о состоянии здоровья, местоположении, времени и т.д. Широкое распространение фитнес браслетов и умных часов привело к тому, что компании производители этих устройств накапливают огромное количество данных о физической активности пользователей гаджетов. Эти данные позволяют определить не только уровень физической активности, но и составить точную план-схему местоположения пользователя в зависимости от времени суток и дня недели. Анализ существующих реализаций фитнес приложений показывает, что система защиты пользовательских данных состоит из следующих компонентов:

- защита локальных данных на мобильном устройстве;
- безопасная передача данных между серверным и клиентским приложением;
- меры, предотвращающие несанкционированный доступ к базе данных и в частности к CRUD-операциям.

В докладе рассмотрены принципы защиты пользовательских данных в фитнес приложениях, проведена их классификация. Проведено ранжирование данных с точки зрения рисков для пользователя и важности для киберпреступника. Проанализированы каналы утечки информации в фитнес приложениях, возможные виды атак и их классификация. Предлагается комплексная система защиты пользовательских данных в фитнес приложении. Для достижения поставленной задачи проведен анализ существующих механизмов защиты пользовательских данных, а также разработан действующий прототип комплексной системы защиты.

Защита пользовательских данных необходима как из соображений информационной безопасности, так и в соответствии с требованиями правовых норм. Предложенные меры обеспечения безопасности данных повышают уровень пользовательского доверия к приложению и сервису в целом.

АНАЛИЗ МЕР БЕЗОПАСНОСТИ И ЗАЩИТЫ КОМПЬЮТЕРНЫХ ИГР ОТ ВЗЛОМА

Вивчар Т.В., к.т.н. Дужий В.И., к.т.н. доц. Пєвнєв В.Я.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков

Индустрия компьютерных игр относится к сфере развлечения и является одной из самых быстроразвивающихся и доходных на рынке информационных технологий. Компьютерные игры вносят значительный вклад в мировую экономику ввиду большого успеха продаж основных игровых систем и игр. По мере развития отрасли возросло количество случаев нарушения авторского права и хищения контента, что привело к необходимости совершенствования методов борьбы с этими явлениями.

За последние три десятилетия методы защиты компьютерных игр прошли несколько этапов развития. На первоначальном этапе использовался подход пошаговой документации. В настоящее время самым широко применяемым методом являются технические средства защиты авторских прав. Другое направление основано на переходе от платформы персональных компьютеров на консоли. Применение облачных игровых технологий является самым успешным решением проблемы, однако нуждается в анализе и оценке возможных угроз.

С появлением новых технологий защиты появляются и новые угрозы, что обуславливает следующие шаги. На данный момент рассмотрены перспективы развития системы предотвращения взлома на ближайшие года. Но до сих пор невозможно определить, будет ли когда-то полностью искоренено игровое пиратство или нет.

В докладе проанализированы этапы развития защиты компьютерных игр. Особое внимание уделено практики использования пиратских версий игровой продукции. Показаны методы обходы водяных цифровых знаков, взлома систем защиты от незаконного копирования. Предлагаются методы борьбы со взломом систем безопасности видеоигр, основанные на использовании распределенных цифровых знаков, ограничении функциональных возможностях используемых игр при несанкционированном доступе.

Большие возможности в защите игровых программ появляются при использовании облачных технологий. В докладе рассмотрены возможные пути организации различного вида атак на игровые программы, защиты, как авторских прав, так и программного кода при использовании современных инфокоммуникационных технологий. а также рассмотрено возможное будущее сферы защиты видеоигр.

ОБЕСПЕЧЕНИЕ БЕЗОПАСТНОСТИ ПОДСИСТЕМЫ КОНТРОЛЯ И ДИАГНОСТИКИ СОСТОЯНИЯ ЧЕЛОВЕКА

Дмитренко М.А., Галькевич А.А., к.т.н. доц. Певнев В.Я.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», г. Харьков

Развитие информационных технологий дало импульс в развитии многих наукоемких производств, в том числе и в медицине. Существующие диагностические комплексы позволяют точно диагностировать любые заболевания. Главным недостатком таких комплексов является их большая стоимость. Поэтому последнее время большое внимание начали уделять малогабаритным, переносным комплексам, которые позволяют произвести диагностику в «полевых» условиях.

Методы диагностирования, которые используются в таких случаях, основываются на традиционных методах народной медицины. Одним из таких методов является диагностирование по пульсу человека.

Пульс – это колебания стенок сосудов, вызванных ритмическими последовательными сокращениями и расслаблениями сердца. В медицине выделяют его артериальную, венозную и капиллярную разновидности. Полная характеристика пульса позволяет получить подробную картину о состоянии сосудов и особенностях гемодинамики (кровотока). Пульс одна из главных характеристик состояния человека.

Для контроля и диагностики состояния человека была разработана подсистема, которая позволяет в реальном времени следить за пульсом человека и выводить эти показания на экран, а также заносить эти показания в локальную и глобальную базу данных. В случае критических показаний предусмотрен автоматический вызов скорой помощи и передача координат местонахождения человека.

Одним из недостатков подобных систем является возможность несанкционированного доступа при использовании стандартных каналов связи. Необходимо принятие специальных мер по недопущению несанкционированного доступа к персональным данным и измеряемых параметров состояния здоровья пациента

В докладе проведен обзор и сравнение существующих подсистем, определены достоинства и недостатки, которые учитывались при разработке подсистемы контроля и диагностики состояния человек. В представленном докладе рассмотрены существующие методы защиты информации. Для подсистемы контроля и диагностики состояния человека был выбран метод для защиты данных при хранении и обращении к ним, который больше всего подходит для медицинских систем. Это повышает надежность и безопасность данной подсистемы.

ОБЗОР СУЩЕСТВУЮЩИХ АЛГОРИТМОВ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ МУЛЬТИВАРИАТИВНОЙ СХЕМЫ ШИФРОВАНИЯ

Евсеева Е.В., д.т.н. проф. Потий А.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», г. Харьков

Достижения квантовых вычислений сформировали новые вызовы для классических криптографических схем. В частности, в соответствии с учетом ENISA, а также, по мнению других исследователей, считается, что схемы цифровых подписей на основе RSA, DSA и даже на основе преобразования точек на эллиптических кривых уже не могут считаться безопасными. В связи с этим в криптографическом сообществе ведется активный поиск новых криптографических примитивов, которые смогут эффективно противостоять алгоритмам, построенным на квантовых вычислениях. Такие алгоритмы относятся к классу постквантовых. Постквантовая криптография – это общее наименование всех криптосистем, которые могут противостоять атакам, опирающимся на квантовые компьютеры. Учитывая актуальность и необходимость создания постквантовых алгоритмов электронной подписи, в этом направлении уже начаты исследования, в определенной степени определены математические основы, на которых могут быть построены постквантовые алгоритмы электронной подписи и ассиметричного шифрования.

В докладе рассматриваются схемы ЭЦП на основе мультивариативных преобразований. К таким схемам относятся:

– Unbalanced Oil and Vinegar (UOV);
– Hidden Field Equations (HFE);
– Hidden Field Equation vinegar (HFEv);
– Rainbow.

Проблема решения мультивариативных алгебраических уравнений относится к классу np-полных задач. Поэтому, можно предположить, что они будут стойкими к квантовым вычислениям. В докладе рассмотрены характеристики алгоритмов цифровой подписи, построенных на основе MQ-криптографии, проведена их классификация по:

– показателям криптографической стойкости;
– показателям технической реализации алгоритмов;
– техно-эксплуатационным требованиям.

Системы цифровой подписи на основе MQ-преобразований вполне могут использоваться в перспективе для замены существующих подписей в публичных приложениях.

ОБЕСПЕЧЕНИЕ КИБЕРЗАЩИТЫ ПРИ УПРАВЛЕНИИ АВТОМАТИЗИРОВАННЫМ КОРМОРАЗДАТЧИКОМ

Галькевич А.А., Кибец Ю.Н., к.т.н., доц. Певнев В.Я.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», г. Харьков

Стремительное развитие информационных технологий кардинально меняет многие производственные циклы, освобождает рабочих от тяжелого монотонного физического труда. Создаваемые устройства, основанные на использование различных процессоров, позволяют более четко выполнять технологические требования при выполнении различных операций. Вместе с тем возникает угроза воздействия на процесс принятия решений за счет несанкционированного вмешательства. Поэтому вопросы обеспечения кибербезопасности становятся одними из главнейших при эксплуатации подобных систем.

В докладе представлены результаты проектирования устройства кормораздачи. Показаны решения, позволяющие в автоматизированном режиме выполнять управление движением, дозированной раздачей кормов, контроль заполнение бака; анализ заряда аккумулятора, управление аварийной сигнализацией; программирование через интерфейс USB; хранение данных в БД.

В качестве основной киберугрозы в докладе рассматривается несанкционированное подключение к каналам связи, осуществление перехвата информации и модификация передаваемых по каналам данных. Для обеспечения киберзащиты данных, передаваемых по указанным каналам связи, предлагается использование средства криптографической защиты.

Для данной системы был рассмотрен «Удаленный доступ по защищенному каналу с использованием криптошлюза». С помощью криптошлюзов можно формировать виртуальные защищенные каналы в сетях общего пользования, гарантирующие конфиденциальность и достоверность информации, организовывать виртуальные частные сети, подключенных к сети общего пользования в единую защищенную виртуальную сеть.

В докладе представлен анализ вариантов специального программного обеспечение, обеспечивающего централизованное управление локальными политиками безопасности VPN-клиентов и криптошлюзов, выявлены их недостатки и показаны преимущества. Представлено разработанное специальное программное обеспечение, использование которого позволяет более надежно обеспечить криптозащиту системы управления объекта от несанкционированного вмешательства.

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ VPN

Литвиненко Б.В., Цуранов М.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», г. Харьков

Стремительное развитие персональной вычислительной техники и широкое распространение технологии VPN привело к тому что не только стационарные компьютеры и ноутбуки, но и планшетные персональные компьютеры и смартфоны поддерживают технологию VPN. Использование данной технологии расширилось с простой возможности удаленного доступа сотрудников к корпоративной сети до средства защиты от перехвата трафика в открытых сетях, а также для доступа к блокируемым в данном регионе ресурсам (проект «Золотой щит» в Китайской Народной Республике, блокировки Роскомнадзора в Российской Федерации). Пользователи крайне редко задумываются о безопасности самого VPN-приложения. По данным исследования специалистов из университета Нового Южного Уэльса и Калифорнийского университета в Беркли из рассмотренных 283 приложений для организации VPN-соединения на базе ОС Android 38% приложений содержат вредоносный код (нежелательная или вредоносная реклама, шпионское ПО), 18% приложений реализуют передачу данных через сервер без шифрования, 16% приложений передают данные не через VPN-сервер, а через других пользователей приложения. Кроме перечисленных проблем в которых виноват недобропорядочный разработчик существуют уязвимости в реализации протоколов VPN. Существуют 4 основные уязвимости реализаций VPN: разрывы VPN-соединения, DNS-утечки, утечки связанные с использованием адресации IPv6, законодательные отличия (если VPN-сервер находится в другой стране).

В докладе рассмотрены основные угрозы при использовании технологии VPN на мобильном устройстве. Проведен анализ существующих уязвимостей технологии VPN и разработаны способы их устранения. Для минимизации найденных уязвимостей создан VPN-клиент для мобильных устройств в котором реализованы необходимые функции безопасности.

Вопрос обеспечения защиты информации для мобильных устройств при использовании технологии VPN стоит очень остро так как технология является широко распространенной, а существующие в текущих реализациях уязвимости сводят на нет все преимущества технологии и могут нести в себе дополнительные уязвимости.

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО ДИСТАНЦИОННОГО УПРАВЛЕНИЯ СИСТЕМАМИ В УМНОМ ДОМЕ

доц. Галькевич А.А., к.т.н., доц. Певнев В.Я., Молодык Е.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», г.Харьков

Большое значение необходимо уделить безопасности системы управления. Любое несанкционированное воздействие может привести к непоправимому урону, вплоть до уничтожения самого умного дома.

Способов воплотить в жизнь идею постоянного поддержания определённого «климата» существует достаточно много. Общее у них одно – это централизованная система управления, в которой каждое действие, включение или выключение определённого модуля расписано с точностью до секунды, а изменение температуры воздуха (как внутри, так и снаружи помещения) даже на одну десятую градуса является поводом для внесения коррективов в работу всей системы.

Подсистема управляет всеми инженерными коммуникациями, которые отвечают за микроклимат, в зависимости от заданных параметров и условий в помещении. При изменении температуры или влажности и в зависимости от того есть ли люди в помещении происходит корректировка, регулирование и поддержание необходимых параметров.

Благодаря автоматизированной подсистеме возможно поддерживать необходимые параметры в зависимости от времени года, наружной температуры, резких климатических и погодных изменений и наличия или отсутствия человека в умном доме. Также автоматизированная подсистема позволяет экономить энергоресурсы.

При интеграции такого рода системы необходимо продумать оптимальный протокол использования, для правильного функционирования системы управления.

Протокол ZigBee это не только гарантированная, устойчивая к помехам, сбоям и отказам передача данных, но и самое главное безопасная передача, что первостепенно для нашей системы.

Ключевым элементом концепции безопасности ZigBee является Центр управления безопасностью.

На этапе формирования или реконфигурации сети центр управления безопасностью разрешает или запрещает присоединение к сети новых устройств. Центром управления безопасностью может являться как координатор сети, так и специально выделенное устройство.

В данном докладе рассмотрена возможность применения протокола ZigBee для гарантированного уровня безопасности в системе управления микроклиматом в умном доме.

ЗАДАЧА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО ДИСТАНЦИОННОГО УПРАВЛЕНИЯ ДЕТСКОЙ ИНТЕРАКТИВНОЙ ИГРУШКОЙ

Галькевич А.А., к.т.н., доц. Певнев В.Я., Семенюк Е.О.
Национальный аэрокосмический университет им. Н.Е.Жуковского «ХАИ», г. Харьков

Интерактивные игрушки-роботы являются одним из важных направлений научно-технического прогресса, в котором проблемы механики соприкасаются с проблемами управления и искусственного интеллекта. Кроме всего того, что присуще обычным игрушкам, их интерактивные родственники умеют общаться с детьми и активно играют с ними – побуждают к действиям, разговаривают, поют, дают обратную связь, меняют свои движения и сигналы, ориентируясь на поведение чада.

Анализ существующих реализаций показывает, что польза от таких игрушек очевидна: интерактивные друзья помогают произносить слова, складывать их в предложения, четче выговаривать. Играя, ребенок учится лучше воспринимать информацию на слух, распознавать предложения, выполнять просьбы. Дети через игровой процесс познают много нового, учатся моделировать различные ситуации, общаться, находить решения, но главное – они будут при этом веселиться и развлекаться.

Разработанная интерактивная игрушка выполняет следующие основные функции: ориентация в пространстве, реагирование на свет, реакция на тактильный контакт, распознавание и воспроизведение звуков. Так же присутствует дистанционное управление и связь с игрушкой, что позволяет родителям всегда знать, где ребенок и чем он занят.

Задача обеспечения безопасности ребенка при контакте с игрушкой напрямую связана с защитой удалённого доступа и управления, защитой персональных данных от несанкционированных действий, и является одной из главных при разработке. Решая эту проблему важно продумать наиболее подходящий модуль организации и передачи данных. GSM-сети характеризуются не только самой широкой распространенностью, но и высокой надежностью и производительностью. С ними удобно работать, из-за маленьких размеров модули легко спрятать, а также родители могут управлять системой игрушки при помощи мобильного устройства.

В предлагаемом докладе рассматриваются возможные подходы к решению задачи обеспечения защищенного удаленного доступа к системе управления игрушки и целостности персональных данных ребенка и его семьи.

МЕТОДЫ ЗАЩИТЫ СИСТЕМЫ УПРАВЛЕНИЯ МОДУЛЬНОЙ ГИДРОПОННОЙ ТЕПЛИЦЕЙ

доц. Галькевич А.А., к.т.н. доц. Певнев В.Я., Суходубова А.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», г. Харьков

Теплица – отапливаемый парник, представляющий собой защитное сооружение для выращивания ранней рассады (капусты, томатов, огурцов, цветов сеянцев, укоренения черенков или доращивания горшечных растений), для последующего высаживания в открытый грунт. Для выращивания растений в теплицах используется несколько способов: гидропоника, система капиллярного полива, аэропоника. В целом, все рассматриваемые системы предоставляют схожие функции, при этом каждым годом они развиваются все больше и больше.

Гидропоника— это способ выращивания растений на искусственных средах без почвы. При выращивании гидропонным методом растение питается корнями не в почве, более или менее обеспеченной минеральными веществами и поливаемой чистой водой, а во влажно-воздушной, сильно аэрируемой водной, среде, способствующей дыханию корней, и требующей сравнительно частого полива рабочим раствором минеральных солей, приготовленным по потребностям этого растения. Гидропонное хозяйство предусматривает управление температурой, влажностью, освещением и водоснабжением в теплице.

При реализации данного проекта была разработана система управления гидропонного хозяйства. Разработанная система позволяет реализовать многоточечный контроль и регулирование температуры, измерение и оценку влажности, управление дозированным поливом, а также автоматизированный процесс подкормки растений. Система реализована на современной элементной базе, предусмотрена возможность энергонезависимой работы при временном отключении источника питания.

В докладе представлен сравнительный анализ существующих способов защиты данных в системах управления модульной теплицей. Особое внимание уделено их недостаткам. Рассмотрены возможные виды несанкционированного воздействия на систему управления.

В докладе детально рассматриваются разработанные методы защиты данных от несанкционированного доступа. Представленные методы позволяют улучшить безопасности данных и повысить надежности стабильной работы подсистемы управления модульной гидропонной теплицей. В докладе представлены таблицы, отражающие результаты натурного эксперимента.

ЗАЩИТА ЭЛЕКТРОННОЙ МЕДИЦИНСКОЙ КАРТОТЕКИ ПАЦИЕНТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

к.т.н. Дужий В.И., к.т.н., доц. Певнев В.Я., Терихова Ю.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», г. Харьков

Двадцать первый век – это эпоха цифровых технологий. В информационной сфере электронные сервисы стремительно завоевали популярность. К ним можно отнести: электронное правительство, электронные услуги, а также электронные библиотеки. Область медицины также не является исключением. Задача перехода от бумажного способа ведения медицинской документации к электронному до сих пор остается актуальной – об этом говорит разнообразие стандартов ведения электронных медицинских записей: стандарты HL7, DICOM и другие. Более того, эта задаче вскоре станет просто необходимой.

Основная задача такой системы ведения медицинских записей состоит в объединении государственных и частных клиник в единую базу, ведении персональной карточки пациента и предоставлении медицинским учреждениям функционального инструмента с целью повышения конкурентоспособности в сфере медицинского обслуживания.

Одним из главных вопросов, возникающих при организации подобных систем, являются вопросы обеспечения безопасности. Двуединая задача обеспечения безопасности включает в себя защиту персональных данных пациентов и обеспечения возможного удаленного доступа к данным.

Обеспечение защиты персональных данных пациентов предполагает обеспечение их конфиденциальности и целостности. Вопросы обеспечения конфиденциальности данных пациентов разработаны достаточно полномасштабно, благодаря достаточно множественным и серьезным работам в области криптографии. В тоже время вопросам обеспечения целостности данных практически не уделяется внимания. Большинство исследований рассматривают методы обеспечения контроля целостности, что не является решением проблемы обеспечения целостности.

В предлагаемом докладе рассматриваются возможные подходы к решению задачи обеспечения целостности персональных данных пациентов, включая возможности удаленного доступа к их электронным медицинским картам, состоящим из истории болезни, результатов анализов, диагнозов врачей, ведения удаленных консультаций, внесения новых схем лечения и сигнальных отметок пациентов.

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ ПРИ ИСПОЛЬЗОВАНИИ БЕСПРОВОДНЫХ СИСТЕМ СВЯЗИ

доц. Галькевич А.А., к.т.н., доц. Певнев В.Я., Чмара А.Г.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», г.Харьков

Актуальным вопросом при использовании беспроводных сетей является их безопасность. Это связано с тем, что прослушивание таких сетей не составляет особого труда. Следует отметить, что существующие методы повышения безопасности ориентированы в основном на сети фиксированной структуры.

Технология Bluetooth была разработана в середине 90-х как средство для подключения к компьютеру беспроводной клавиатуры. Сегодня Bluetooth обеспечивает взаимодействие беспроводных телефонных гарнитур с телефонами и компьютерами, и это только одна из сфер применения данной технологии. Устройства Bluetooth, как и изделия, реализующие родственную и более известную технологию беспроводной связи Wi-Fi, подвергаются многочисленным атакам хакеров.

За последние годы в средствах массовой информации появился целый ряд сообщений о лазейках в системе безопасности Bluetooth. Правда, самые сенсационные обвинения касаются не самого стандарта Bluetooth, а конкретных реализаций стека Bluetooth и служб (Bluebugging, Bluetracking, Bluestumbling и т.д.).

Когда канал связи между двумя устройствами не защищен, злоумышленник может с легкостью выдать себя за одно из устройств и направить на другое устройство фальсифицированные пакеты. Еще одна проблема, типичная для определенного класса устройств Bluetooth, таких как не наделенные пользовательскими интерфейсами беспроводные телефонные гарнитуры, — это использование хакерами фиксированных общих ключей (которые часто бывают общедоступными). Пожалуй, наибольшее беспокойство вызывает то обстоятельство, что технология Bluetooth не обеспечивает анонимности пользователей. Если на устройстве активизированы средства Bluetooth, следует исходить из того, что конфиденциальные данные могли стать достоянием третьих лиц. Радиопередатчиками Bluetooth оснащаются все новые категории устройств, и в дальнейшем популярность этого стандарта будет только возрастать.

В представленном докладе проводится анализ безопасности работы Bluetooth, рассматривается несанкционированные воздействия на Ваше устройство, методы защиты от различных атак и способы защиты информации от НСД.

ПУТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ СИСТЕМЫ АВТОМАТИЧЕСКОГО ПОЖАРОТУШЕНИЯ

Галькевич А.А., к.т.н. доц. Певнев В.Я., Чумак А.М.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», г. Харьков

Автоматизация различных элементов быта является одной из базовых идей построения «умного дома». В таких системах необходимо уделять большое внимание кибербезопасности, т.к. внешнее воздействие на датчики или исполнительные устройства могут привести фатальным последствиям.

Особое внимание следует обратить на критические системы, к числу которых относится система автоматического пожаротушения. Данная система предлагает использование различных типов датчиков и исполнительных механизмов, задача которых состоит в постоянном отслеживании определенных параметров изменяемой среды внутри помещения и своевременное применение мер ликвидации возгорания.

В докладе представлен анализ, предлагаемых на рынке реализаций систем автоматического пожаротушения, показано, что исследуемая система имеет два возможных пути проникновения. Первый путь- это сеть, связывающая беспроводные датчики, и второй - система оповещения, сообщающая владельцу о критической ситуации по мобильному каналу посредством SMS-сообщения.

При проведении поиска возможных вариантов противодействия несанкционированному воздействию на систему пожаротушения, основываясь на экономической целесообразности их применения, были обнаружены такие пути решения поставленной задачи.

Обеспечение кибербезопасности сети достигается за счет использования сетевых протоколов верхнего уровня под названием ZigBee. Данные протоколы на этапе формирования или реконфигурации разрешают или запрещают присоединение к сети новых устройств. Данное свойство позволяет полностью исключить несанкционированное подключение неидентифицированных устройств к системе пожаротушения. В контексте обеспечения работы беспроводных датчиков, ZigBee имеет ряд и других свойств, которые позволяют обеспечить заданный уровень защиты. Для решения проблемы оповещения владельца по SMS-сообщению, было решено использовать стандарт мобильной сотовой связи GSM, который хоть и проигрывает технологии CDMA по уровню защищенности и энергопотребления оборудования, но в тоже время имеет ряд готовых решений как операторского, так и потребительского оборудования.

МЕТОДЫ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАНОГО ДОСТУПА К СИСТЕМЕ УПРАВЛЕНИЯ АДАПТИВНОЙ ПОДВЕСКОЙ АВТОМОБИЛЯ

доц. Галькевич А.А., к.т.н. доц. Певнев В.Я., Яскевич С.С.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», г.Харьков

Под термином «адаптивная» понимается подвеска, параметры которой могут изменяться во время эксплуатации. Электронная система управления в составе адаптивной подвески позволяет изменять параметры автоматически. А именно степень жесткости деформирующего устройства (пневмо-подушки). Под степенью жесткости деформирующего устройства понимается быстрота затухания колебаний, которая зависит от сопротивления устройств (пневмо-подушек).

Существует три основных адаптивных системы. Адаптивная пневматическая подвеска является опережающей системой по плавности хода. Отличается отсутствием пружин, их роль выполняют резиновые баллоны, наполненные воздухом. При помощи электронно-управляемого пневмо-привода можно отдельно работать с каждой пневматической стойкой, регулируя высоту каждой части кузова.

Адаптивная гидро-пружинная подвеска сопровождаться установкой специальных гидравлических цилиндров. Основываясь на данных от сенсоров, следящих за кузовом во всех направлениях, электроника корректирует положение каждой гидро-пружинной стойки. Такая система исключает крены кузова при различных условиях движения.

Адаптивная подвеска на основе адаптивных задних рычагов, то есть активный контроль геометрии подвески. В такой конструкции для каждого заднего колеса предусмотрена пара дополнительных рычагов с электроприводами, которые при повороте, торможение, начинают работать: электроника собирает множество данных, а затем доворачивает то колесо, которое в этот момент находится под нагрузкой.

В докладе представлен сравнительный анализ существующих способов защиты данных в системах управления адаптивной подвеской. Особое внимание уделено их недостаткам. Рассмотрены возможные виды несанкционированного воздействия на систему управления.

В докладе детально рассматриваются разработанные методы защиты данных от несанкционированного доступа. Представленные методы позволяют улучшить безопасности данных и повысить надежности стабильной работы системы управления адаптивной подвеской автомобиля. В докладе представлены таблицы, отражающие результаты натурного эксперимента.

ВРАЗЛИВІСТЬ СИСТЕМИ WORDPRESS

Антонюк В.В., к.ф-м.н., доц. Черних Е.П.
Національний технічний університет «ХПІ», Харків

На сьогоднішній день WordPress – це найпопулярніша та зручна блог-платформа для публікації статей та управління ними, на якій базується величезна кількість різних сайтів. Від загального числа сайтів, які використовують CMS-движки, її частка становить 60,4%. Відповідно зі статистикою 67,3% сайтів базується на останній версії даного програмного забезпечення. На жаль, базові налаштування не забезпечують достатнього рівня захисту. За тринадцять років існування веб-движка в ньому було виявлено 242 уразливості різного роду (без урахування вразливостей, знайдених в сторонніх плагінах і темах).

Плагін Jetpack – один з найпопулярніших для WordPress. Він включає велику кількість модулів (від створення галерей і розсилки в соціальні мережі до захисту від перебору паролів і підрахунку відвідуваності). За даними директорії WordPress.org, Jetpack має майже 25 мільйонів завантажень, і активний на понад 1 мільйон WordPress сайтів.

Дослідники з фірми веб-безпеки Sucuri знайшли «міжсайтовий скриптинг» (XSS), через який уразливості піддаються всі випуски Jetpack, починаючи з версії 2.0. Проблема розташована в модулі Shortcode Embeds, який дозволяє користувачам вбудовувати зовнішні відео, зображення, документи, твіти та інші ресурси в свій контент. Він може бути з легкістю використаний для введення шкідливого JavaScript-кода в коментарі. Так як JavaScript-код повторюється, він буде виконуватися в браузерах користувачів кожен раз, коли вони переглядають цей шкідливий коментар. Наприклад, він може використовуватися, щоб вкрасти ідентифікаційні куки, включаючи сеанс адміністратора; перенаправити відвідувачів до експлойтів або ввести спам пошукової оптимізації (SEO).

Для усунення цієї вразливості команда безпеки проекту WordPress скористалась механізмом автоматичних оновлень в ядрі WordPress, і за допомогою нього оновила Jetpack до останньої версії (в рамках встановленої гілки) на всіх сайтах з подібною підтримкою. Так само вчинили ряд хостинг-провайдерів.

БЕЗПЕКА МОБІЛЬНИХ ДОДАТКІВ

Бреславець О.Ю., к.ф-м.н., доц. Черних О.П., д.т.н., проф. Носков В.І., Гугнін В.М.
Національний технічний університет «ХПІ», Харків

У наш час використання мобільних телефонів стало повсюдним і повсякденним. Завдяки можливостям мобільних додатків, швидкому зростанню обчислювальної потужності смартфонів та все зростаючої доступності мобільних пристроїв програмне забезпечення для смартфонів вимагає все більше часу на тестування та більшої відповідальності у розробці.

З ростом популярності мобільних додатків у користувачів зростає їх популярність і у зловмисників. Додатки на кожній платформі мають як свою специфіку написання, так і свої специфічні загрози, реалізація яких може призвести як до крадіжки особистих даних, в тому числі банківських, так і до проникнення в корпоративну мережу.

Основні проблеми безпеки пов'язані з тим, що різноманітність ОС для мобільних пристроїв дуже велика, так як і кількість їх версій в одному сімействі.

Були розглянуті уразливості, які найбільш часто зустрічаються та включені в список OWASP Mobile Top Ten Risks. Основними проблемами, які легко усуваються на етапі розробки, є:

– небезпечне зберігання даних;
– недостатній захист каналів передачі інформації;
– слабка авторизація та аутентифікація;
– небезпечне управління сесіями.

Для захисту мобільних додатків від вразливостей необхідно:

– не зберігати дані на SD карті;
– вимикати логування;
– переглядати конфігураційні файли додатків користувача на предмет забутих даних.

Таким чином, швидке розширення функціоналу веде за собою велику складність і меншу захищеність мобільних пристроїв. Розглянуті проблеми переважно виникають при неправильній організації процесів розробки і тестування.

МЕТОДИ ЗАХИСТУ ВІД СНІФІНГУ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Ковтун Р.О., к.ф-м.н., доц. Черних О.П.
Національний технічний університет «ХПІ», Харків

У сучасних комп'ютерних мережах існує ризик сніфінгу (перехоплення та аналізу мережевого трафіку сторонніми особами). Основними методами захисту від сніфінгу є:

– аутентифікація;
– комутована інфраструктура;
– антисніфери;
– криптографія.

Аутентифікація. Прикладом є система одноразових паролів, де необхідно мати «токен» (апаратний або програмний засіб, що генерує унікальний одноразовий пароль). Якщо хакер дізнається даний пароль за допомогою сніфера, то ця інформація буде марною, оскільки в цей момент пароль вже буде використаний. Цей спосіб боротьби зі сніфінгом ефективний тільки в випадках перехоплення паролів.

Комутована інфраструктура. Ще одним способом боротьби зі сніфінгом пакетів є створення комутованої інфраструктури. Якщо, наприклад, у всій організації використовується комутований Ethernet, хакери можуть отримати доступ тільки до трафіку, що надходить на той порт, до якого вони підключені. Комутована інфраструктура не усуває загрози сніфінгу, але помітно знижує його доцільність.

Антисніфери. Даній спосіб боротьби зі сніфінгом полягає в установці апаратних або програмних засобів, які розпізнають сніфери, що працюють у вашій мережі. Антисніфери вимірюють час реагування хостів і визначають, чи не доводиться хостам обробляти зайвий трафік.

Криптографія. Це найефективніший спосіб боротьби зі сніфінгом пакетів. Хоча він не запобігає перехопленню і не розпізнає роботу сніферів, але робить цю роботу марною. Якщо канал зв'язку є криптографічно захищеним, то хакер перехоплює не вихідне повідомлення, а зашифрований текст (незрозумілу послідовність бітів). Для створення захищеного зв'язку між пристроями використовуються протоколи, IPSec, SSH (Secure Shell) і SSL (Secure Socket Layer).

Для підвищення ефективності захисту від сніфінгу у комп'ютерних мережах можна використовувати перераховані методи разом.

ОТСЛЕЖИВАНИЕ ПОИСКОВЫХ РОБОТОВ

Стрельцов В.В., к.ф-м.н., доц. Черных Е.П.
Национальный технический университет «ХПИ», Харьков

Поисковые роботы («веб-пауки») − программы, являющиеся составной частью поисковой системы. Их принцип действия аналогичен обычным браузерам и предназначены они для перебора страниц Интернета с целью занесения информации об их посещениях в базу данных поисковика.

Владельцы поисковых машин нередко ограничивают глубину проникновения паука внутрь сайта и максимальный размер сканируемого текста, поэтому чересчур большие сайты могут оказаться не полностью проиндексированными поисковой машиной. Статистика посещений пользователей приводится обычно для распространенных сайтов. Для получения аналогичной информации с еще нераскрученных сайтов лучше написать свой скрипт. Также страницы могут посещать вредоносные боты. Установкой пароля на странице либо требованием заполнить регистрационную форму перед тем, как получить доступ к содержимому, не всегда можно обеспечить защиту сайта.

SEO-специалист может выполнить проверку на посещение сайтов поисковыми роботами, а также зафиксировать информацию об индексации сайта в «всемирной паутине». При анализе содержимого страницы, он сохраняет его в некотором специальном виде на сервере поисковой машины, которой принадлежит, и отправляется по ссылкам на следующие страницы.

Для решения данной проблемы был предложен подход – разработка программного модуля (скрипта), с помощью которого можно отследить визиты поисковых роботов. Скрипт будет содержать необходимую информацию: дату посещения, имя бота, IP-адреса бота и страницы, которые он посетил.

Данный подход позволит контролировать индексацию последних изменений страниц на определенном сайте и определить какие роботы посещали данный сайт. Это, в свою очередь, приведет к повышению эффективности индексации сайта.

Программная реализация может быть выполнена с помощью языков программирования PHP или JS.

АНАЛИЗ ОСНОВНЫХ ПОДХОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В MPLS СЕТЯХ

к.т.н., Горюшкина А.Э., к.т.н., доц. Угрин Д.И.
Национальный технический университет «ХПИ»

Проведенные исследования показали, что традиционные средства и методы борьбы с киберугрозами основаны на принципе установки разнообразных “информационных барьеров”. Средства и методы построения виртуальных частных сетей (VPN) отличаются от традиционного подхода к защите сетей на основе “информационных барьеров”. Они позволяют строить выделенные, или частные, сети на базе разделяемой сетевой инфраструктуры и таким образом реализовать упреждающую, превентивную стратегию защиты сети.

Условно сети VPN можно разделить на три основные группы по способу реализации: традиционные сети VPN на основе криптографических сервисов шифрования и аутентификации данных, реализованных в таких протоколах, как IPSec; традиционные сети VPN на основе разделения каналов второго уровня (Frame Relay, ATM, Ethernet VLAN); сети VPN на основе разделения таблиц коммутации и маршрутизации (MPLS VPN).

Средства реализации VPN первой и второй групп часто имеют серьезные недостатки. Потенциально слабая криптография и ошибки в ее реализации, а также частные схемы распределения ключей приводят к нарушению целостности, доступности или конфиденциальности передаваемых данных. Также к минусам подобных средств следует отнести сложность в управлении сетью и схемой распределения ключей при больших масштабах и географической распределенности VPN; потенциальные проблемы при работе VPN через межсетевые экраны (например, в случае использования алгоритмов трансляции сетевых адресов (NAT) с протоколом IPSec); частую несовместимость различных реализаций VPN.

Для дальнейших исследований перспективной представляется третья группа реализации, в которой сервисы L2 VPN, организованные на основе технологии MPLS, лишены вышеперечисленных недостатков. Сервис-провайдер не обязан содержать выделенную L2-сеть для того, чтобы поддерживать такой сервис. Технологии MPLS L2 VPN позволяют “прокладывать” каналы второго уровня через разделяемую опорную сеть, по которой, помимо MPLS VPN, работают традиционные IP-сервисы.

ИССЛЕДОВАНИЯ СХЕМ ЗАЩИТЫ ИНТЕРНЕТА ВЕЩЕЙ

Семенова А.С., Бартош М.В.
Национальный технический университет «ХПИ», Харьков

Интернет вещей (IoT) одно из новых направлений современных информационных технологий обеспечивает повсеместную связь между различными устройствами. Однако, функциональность и операции IoT в значительной степени зависят от базовой структуры подключения к сети. Данный факт неизбежно вызывает проблемы безопасности в связи с возможностью незаметного подключения и автоматизированной интеграции между к различным видам приложений. Например, злоумышленник может использовать взаимосвязанные устройства для распространения вредоносных программ. Таким образом, эффективные и действенные механизмы защиты имеют первостепенное значение для обеспечения безопасности IoT.

Проблема усугубляется разноодностью аппаратно-программных средств обеспечивающих функционирование IoT. Поэтому именно в последнее время этому вопросу начали уделять большое влияние. Так на базе Стэндфордского университета США была сформирована группа специалистов для разработки унифицированных предложений защиты данных в IoT. А департамент США по энергетике (DOE) приступил к разработке предложений защиты от активных атакна уровне топологии.

В докладе представляя сложные соединения в IoT в виде сети, исследуются сетевые уязвимости IoT к различным схемам атаки. Исследуются три схемы защиты: внутренняя топологическая схема защиты, комбинированная схема защиты, и схема последовательной защиты. Кроме того, путем исследования взаимосвязи между злоумышленником и субъектом активной защиты, как игры двух игроков с нулевой суммой, представлены предложения, максимизирующие выигрыши субъектов активной защиты.

Результаты продемонстрированы с помощью графиков данных.

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНА СИСТЕМА КОНТРОЛЮ ТА БЕЗПЕКИ В РОЗПОДІЛЬНИХ ЕЛЕКТРИЧНИХ МЕРЕЖАХ

Конєв В. В.
Український державний університет залізничного транспорту, Харків

Великий інтерес нині викликають системи енергоспоживачів, що фізично розподілені на великій території. До таких систем належать розподільні електромережі напругою до 1000 В, які є ключовим компонентом у процесі транспортування і розподілу електроенергії споживачам. Для стійкої та ефективної роботи таких мереж потрібні з одного боку моніторинг стану і достовірне управління розподільними електромережами, з іншого боку - суворий облік енергоресурсів, а також забезпечення електробезпеки.

Існуючі інформаційно-вимірювальні системи мають ряд істотних недоліків: відсутня інформація про окремих споживачів у реальному часі; відсутні оперативні баланси відпущеної і спожитої електроенергії; відсутня діагностика за визначенням місць пошкоджень і кількості втраченої електроенергії.

У зв'язку з цим видається актуальним створення єдиної комп'ютеризованої інформаційно-вимірювальної системи (ІВС) контролю ізоляції, обліку несанкціонованого відбору електроенергії і контролю режимів роботи мережі з використанням пристрою для контролю струмів, яка поєднує функції диспетчерського управління та обліку енергоспоживання і забезпечує безперервний автоматизований збір і передачу інформації про величину струму.

В доповіді розглянуті пропозиції щодо створення інформаційно-вимірювального комплексу для розподіленого контролю ізоляції мережі, адресного обліку відбору потужності споживачами і забезпечення реального моніторингу розподільних електричних мереж.

ОБЧИСЛЮВАЛЬНІ РЕСУРСИ БАЗОВОЇ МЕРЕЖІ ГЕТЕРОГЕННОЇ РОЗПОДІЛЕНОЇ СИСТЕМИ

Бульба С.С.
Национальный технический университет «ХПИ», Харьков

Стрімкий розвиток сучасної науки призводить до постійного збільшення та ускладнення обчислювальних задач у сучасному світі. Тому постає необхідність в створенні систем, які зможуть задовольнити необхідні розрахункові потреби. Одним з пріоритетних напрямків вирішення цієї проблеми є створення композитних додатків (КД).

Для представлення математичної моделі процесу припустимо, що всі доступні обчислювальні ресурси (ОР) існуючого КД представляють собою деяку множину доступних КД ресурсів , яка складається з підмножин різних типів ресурсів. В свою чергу під типом ресурсу ми будемо розуміти таке:

- персональний комп'ютер з певними технічними характеристиками (CPU/GPU, RAM, HDD) що є одиничним обчислювальним блоком;
- локальну мережу, створену з набору персональних комп'ютерів, кожен з яких має однакові характеристики (CPU/GPU, RAM, HDD);
- кластери, складові яких мають однакові характеристики (CPU/GPU, RAM, HDD);
- грід-мережу.
- належність кожного ресурсу до одного типу визначається в залежності від таких факторів як:
- однакові технічні характеристики, час передачі даних між ресурсами одного типу;
- однакові операційні системи або прикладне ПЗ, однакова вартість використання.

Визначення типу ресурсу дає змогу точніше сформулювати методи захисту КД від негативного впливу зовнішніх факторів.

МЕТОД БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ ДАНИХ

Серко І.С.
Національний технічний університет «ХПІ», Харків

Питання оптимального розміщення комп'ютерів та маршрутизаторів в захищених інформаційних мережахз метою отримання найприйнятнішого трафіку і захисту передачі інформації є актуальною задачею як при створенні нової мережі, так і при оптимізації існуючої. Для оптимальної побудови захищеної інформаційної мережі інтегрального обслуговування, що включає, окрім головного сервера, багато локальних серверів, маршрутизаторів та десятки чи сотні робочих комп'ютерів, зручно застосовувати теорію графів. При цьому комп'ютери та маршрутизатори приймають як вершини, а лінії зв'язку – як ребра. Переважно основним критерієм оптимальності є сумарна довжина каналів зв'язку і оптимальною структурою – найкоротша обчислювальна мережа без петель.

Слід враховувати особливості роботи захищених мереж інформації. Кожний окремий комп'ютер, що входить до мережі может потребувати передачі чи отримання інформації в довільний час і з більшою чи меншою періодичністю. Тому не можна завжди розглядати задачі розміщення комп'ютера в мережі, коли попит на обмін інформацією у вершинах графа заданий як детерміновани числа.

Даний апарат зручно використовувати при вирішенні задачі про оптимальне розміщення пунктів комутації та обслуговування в мережах, де сума найкоротших відстаней від пункту передачі до пункту отримання інформації повинна бути мінімальною.

Оптимальне у вказаному значенні місце розміщення пунктів обслуговування називається медіаною графа.

ШИФРУВАННЯ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ЛАНЦЮГА НЕЛІНІЙНИХ ОСЦИЛЯТОРНИХ НЕЙРОНІВ

д.т.н., проф. Литвин[1] В.В.; д.ф.-м.н., проф. Пелещак[2] Р.М.; Пелещак[1] І.Р.
[1]Національний університет «Львівська політехніка», м. Львів;
[2]Дрогобицький державний педагогічний університет ім. І.Франка, м. Дрогобич Львівської області

У сучасній практичній криптографії використовують методи захисту з використанням ключа. Їх поділяють на два види: симетричні (алгоритми з секретним ключем) та асиметричні (алгоритми з відкритим ключем).

У даній роботі запропонована модель шифрування інформації на основі ланцюга нелінійних осциляторних нейронів виду Ван-Дер-Поля:

$$X_k'' + \mu_k \left[X_{\alpha k}^2 - p_k^2 \left(N_{0k}, N_{ck} \right) \right] X_{\alpha k}' + \omega_{0k}^2 X_{\alpha k} = f_{k-1}\left(\omega(t) \right), \quad (1)$$

де $k = 1, 2, ..., N$ - номер нейрона, $p_k^2 \left(N_{0k}, N_{ck} \right) = p_{0k}^2 \cdot \tanh\left(\frac{N_{0k} - N_{ck}}{\sigma_k^2} \right)$ - параметри амплітуд нейронів; N_{0k}, N_{ck} , - число імпульсів, які приходять на k -й нейрон, порогове значення імпульсів k -го нейрона та дисперсія відповідно; ω_{0k}^2 - власна частота k -го нелінійного осциляторного нейрона; $f_{k-1}\left(\omega(t) \right)$ - вхідний сигнал, який поступає на k - й нейрон; $X_{\alpha k} = X_k + \sum_{j=1}^{N} \lambda_{jk} X_j$, $\alpha = 1, 2, ..., N$, λ_{jk} - синаптичні зв'язки між нейронами.. Нелінійні осциляторні нейрони мають власну динаміку і здатні генерувати імпульси за відсутності зовнішніх сигналів при $N_{0k} \geq N_{ck}$.

Проведений аналіз зашифрованого, за допомогою ланцюга нелінійних осциляторних нейронів(1), інформаційного повідомлення показав, що ця модель має вищу ступінь захищеності інформації порівняно з існуючими.

ЭФФЕКТИВНОСТЬ БЕЗОПАСНОЙ КОНСТРУКЦИИ ХЕШ-ФУНКЦИИ MERKLE-DAMGARD «SHOUP»

Сапожкова А.М.
Харьковский национальный университет радиоэлектроники, Харьков

В данной работе рассмотрено два возможных подхода по улучшению существующих схем создания хэш-функций, принимающие на вход сообщения произвольной длины. Вводится множество функциональных классов, которые включают в себя универсальные однонаправленные хэш-функций и стойкие к коллизиям хеш-функции. Для некоторых из этих классов эффективно (с короткими ключами) комбинировать уже существующие схемы. Также, доказывается, что схема Shoup является наиболее эффективной составной схемой для универсальных однонаправленных хэш-функций и в настоящее время наиболее оптимальна.

В погоне за эффективностью и доказуемо безопасной конструкцией практических криптосистем, появилось несколько базовых примитивов как полезные блоки строения этих криптосистем. Два из них - стойкие к коллизиям хэш-функции (CRHFs) и универсальные однонаправленные хэш-функции (UOWHFs).

При сравнении сложности в теоретическом смысле систем, UOWHF считается более слабым примитивом, чем CRHF. Практические криптосистемы в некоторых случаях эффективнее построить на более слабых примитивах, которые легко составляются. С тех пор как UOWHFs - не безусловно безопасный примитив, предположение, что определенные семьи (ответвления) функций UOWHF могут быть более вероятностными, чем предположение об их устойчивости к коллизиям.

Во многих приложениях удобно использовать семейство UOWHFs или CRHFs, например, набор функций, которые проецируют битовые строки разной длины в фиксированную длины строку. Проблема в том, чтобы сконструировать такое семейство при данной единственной UOWHF или CRHF, которые являются типичным случаем, когда один начинает с готовой функции, например, MD5 или SHA-1. Для CRHFs широко распространен безопасный и эффективный метод конструкции Merkle-Damgard. Удивительно, но эти конструкции не применяются к UOWHFs. Для построения семейства UOWHF лучший метод на сегодняшний день - Shoup.

В этой работе описывается область применения конструкции Merkle-Damgard, вводя понятие непрерывности примитивов, которая заключается между CRHF и UOWHF. Доказывается, что конструкция Shoup является оптимальной в некоторых ограниченных моделях вычислений. Оптимальность результата - главный вклад в работу.

СТАТИЧЕСКОЕ ДЕТЕКТИРОВАНИЕ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

к.т.н., Гавриленко С.Ю., Саенко Д.Н.
Национальный технический университет «ХПИ», Харьков

На протяжении последних десятилетий представление специалистов и пользователей о том, как должен выглядеть и работать «идеальная» антивирусная система, менялось. В общем и целом, процесс этого изменения можно представить, как раздельное развитие, конкуренцию и синтез двух концепций: статическое и динамическое детектирование вирусов

Первая группа подходов и методов, включает поиск сигнатур, расчет контрольных сумм, вычисление коэффициентов «похожести», эвристический анализ совокупностей разнообразных признаков.

Однако не менее эффективной разновидностью антивирусной защиты является детектирование вирусов в процессе их работы по характерной последовательности выполняемых действий.

В работе представлены результаты статического анализа 450 упакованных и не упакованных вирусов типа Worm, 3418 не упакованных вирусов типа Trojan, 3500 не упакованных вирусов типа Backdoor с целью выявления закономерностей, связанных с наличием определенных строк импорта и других строк в файле.

Разработанное приложение позволило проанализировать импорт файла и PE- структуру файла.

Полученные результаты позволили выделить наиболее часто используемые API-функции и строки, присущие данному типу вирусов, подсчитать их процентное соотношение

Было также проанализированы 690 безопасных приложений, выделены наиболее часто используемые API функции, подсчитано их процентное соотношение.

Результаты анализа наиболее часто используемых API-функций:

GetModuleHandleA, GetModuleFileNameA, WriteFile, GetModuleHandleA, GetProcAddress, RegCloseKey.

Полученные результаты позволили выделить совокупность строк 78 и API-функции, присущих данному типу вирусов и сформировать его сигнатуру. Полученные данные могут быть использованы в дальнейшем для построения экспертной системы.

ДВОФАКТОРНА АУТЕНТИФІКАЦІЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ЕЛЕКТРОНОГО ЦИФРОВОГО ПІДПИСУ

Резанов Б.М., Анциферова О.О., Камчатна-Степанова К.В.
Национальный технический университет «ХПИ», Харьков

Проведені дослідження і аналіз літератури показали, що всі криптосистеми, що функціонують на принципах використання відкритого / закритого ключа, повністю залежать від захищеності закритих ключів і даних, необхідних для їх формування. Відомо, що закритий ключ ЕЦП може зберігатися на комп'ютері користувача і бути захищений локальним паролем. Однак такий спосіб має ряд недоліків. Зокрема користувач повністю прив'язаний до комп'ютера при формуванні підпису, і в той же час безпека закритого ключа повністю залежить від безпеки самого комп'ютера.

Аналіз сучасних розробок в області аутентифікації показав, що більш надійною альтернативою зберігання закритого ключа є смарт-карта. При цьому така смарт-карта повинна бути оснащена захистом від несанкціонованого доступу (НСД).

Проведені дослідження показали, що одним з ефективних механізмів захисту смарт-карт від несанкціонованого доступу є процедура двофакторної аутентифікації.

Аналіз літератури показав, що в даний час існує ряд сучасних розробок і практичних реалізацій протоколів, програмних продуктів і цифрових пристроїв, що виконують функції двофакторної аутентифікації. Однак вони не позбавлені недоліків. Також одним з основних недоліків практично усіх подібних систем є відсутність контролю цілісності даних (відсутність механізмів контролю за підробкою), та складність мультиагентного адміністрування.

З іншого боку будь-яке ускладнення процедур двофакторної аутентифікації призводить до значного збільшення вартості продуктів. Тому актуальною стає задача розробки і реалізації процедур двофакторної аутентифікації на основі існуючих телекомунікаційних рішень. Це може дозволити знизити собівартість продукту і забезпечити якісний рівень захисту ЕЦП.

В доповіді наведено процедури двофакторної аутентифікації для забезпечення захисту електроного цифрового підпису.

ЗАГРОЗИ КЛЮЧАМ ТА КЛЮЧОВИМ ДАНИМ В СЕРЕДОВИЩІ ХМАРНИХ ОБЧИСЛЕНЬ ТА ПРОПОЗИЦІЇ З ЗАХИСТУ ВІД НИХ

Ананенков А.І.
Харківський національний університет радіоелектроніки, Харків

Підвищений інтерес до впровадження хмарних сервісів та їх активне застосування зумовило появу нових задач захисту інформації з урахуванням особливостей функціонування хмарного середовища.

В середовищі хмари відносно ключових даних можуть існувати та реалізовуватись зі сторони порушника такі загрози:

– компрометація ключів та ключової інформації;

– несанкціоноване знищення ключів та ключової інформації;

– перехоплення та запам'ятовування ключів та ключової інформації;

– нав'язування помилкових або хибних ключів та ключової інформації;

– нав'язування слабких ключів або напів-слабких ключів;

– підміна ключів або ключової інформації;

– отримання несанкціонованого доступу до ключів чи ключової інформації;

– отримання можливості несанкціонованого використання ключів

На основі аналізу стану та вимог відносно безпечності управління ключами зі сторони нормативно-правових документів та стандартів, механізми захисту конфіденційних, особистих та відкритих ключів користувача від виявленої множини загроз, пропонується до використання для забезпечення високого рівня безпеки, тобто високого рівня ймовірностей реалізації загроз в середовищі хмарних обчислень, комплексу технічних, організаційних та організаційно-технічних заходів та засобів, а саме:

– на рівні користувача захищених з необхідним рівнем безпеки ключових носіїв;

– на рівні каналів зв'язку між користувачем та хмарою захищених каналів зв'язку з взаємною автентифікацією сторін та стійкістю вищою за стійкість ключів, що передаються;

– на рівні сервісів ідентифікації, автентифікації, авторизації та керування правами доступом надійних протоколів автентифікації з стійкими криптографічними алгоритмами, а також методів багатофакторної автентифікації.

АНАЛИЗ АТАК ТИПА МЕЖСАЙТОВЫЙ СКРИПТИНГ И СРЕДСТВ ЗАЩИТЫ ОТ НИХ

Арчакова А.И.
Харьковский национальный университет радиоэлектроники, 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.

ВОЗМОЖНОСТИ ПРИМИНЕНИЯ КВАНТОВЫХ КОМПЬЮТЕРОВ В КИБЕРБЕЗОПАСНОСТИ

Назарук Р.Р.
Харьковский национальный университет радиоэлектроники, Харьков

Уже давно перспектива появления полноценного квантового компьютера будоражит умы ученых и заинтересованных людей из области криптографии. Ведь появление компьютера, способного решать сколь угодно сложные задачи, ставит под сомнение существование криптографии в том виде, в котором она есть сейчас. Криптографические протоколы с открытым ключом перестанут иметь смысл, т.к. односторонние функции, строго говоря, перестанут быть односторонними из-за достаточно быстрого вычисления обратных к ним функциям на квантовых компьютерах.

Например, алгоритм Шора позволяет разложить натуральное число n на простые множители за полиномиальное от log(n) время, что делает алгоритмы, основанные на проблеме факторизации числа, такие как RSA, бесполезными.

Как ни странно, спасение телекоммуникаций от квантовой угрозы лежит в той же сфере, где и сама угроза. Связь, основанную на передаче единичных микрочастиц, по идее невозможно прослушивать, поскольку законы квантовой физики не позволяют измерить параметры микрочастицы, не исказив их. Это явление, известное как принцип наблюдателя, в теории устраняет основную проблему «классической» связи — возможность прослушивания. Попытка прослушать сигнал искажает сообщение.

Поэтому квантовые криптосистемы могут использовать «квантовую» линию связи для передачи одноразового ключа шифрования, который, в свою очередь, применяется для шифровки сообщения и трансляции по обычной линии связи.

ФИШИНГ АТАКИ КАК ВИД ОБМАНА В КИБЕРПРОСТРАНСТВЕ

Невструев М.В, Пасека И. В.
Харьковский национальный университет радиоэлектроники, Харьков

В связи с бурным развитием информационных техноголий и все более активным их участием о всех сферах общественной жизни растет и количество людей, желающих поживиться на этом. Киберпреступность сегодня обретает все большие масштабы и количество желающих поживиться на неосторожности и некомпетентности «домохозяек» растет столь же бурно, как и разнообразие изощрённых методов наживы.

Одним из таких методов является «Фишинг-атака».

Phishing-атаки. Phishing (фишинг) - процесс обмана или социальная разработка клиентов организаций для последующего воровства их идентификационных данных и передачи их конфиденциальной информации для преступного использования. Преступники для своего нападения используют spam-сообщения или компьютеры-боты. При этом размер компании-жертвы не имеет значения; качество личной информации полученной преступниками в результате нападения, имеет значение само по себе.

Приведем пример фишинг-атаки: Пользователь получает электронную почту от support@administrator.com (адрес - подменен) со строкой сообщения «модификация защиты», в котором ее просят перейти по адресу www.user_verify.info (имя домена принадлежит нападавшему, а не банку) и ввести его банковский PIN-код.

Чтобы противостоять такому виду атак, важно прежде всего осознавать все «подводные камни» которые могут поджидать пользователя в киберпространстве, для возможности дальнейшего противодействия(иногда методом игнорирования) их. Так же, такого рода клиенты и бот-нэты должны в предельно короткие сроки выявляться, а их деятельность пресекаться. Важно дать пользователю понимание о необходимости использования исключительно проверенных ресурсов, а так же о необходимости регулярного обновления базы сигнатур антивирусных программ. Т.е. необходимо понимание того, что основной вклад в обеспечение собственной безопасности лежит на плечах самого пользователя.

ОРАНІЗАЦІЙНО-ТЕХНІЧНІ МЕТОДИ ОБМЕЖЕННЯ ДОСТУПУ ДО СЕРВЕРУ

Скибенко М.С.
Харківський національний університет радіоелектроніки, Харків

В роботі розглянуто та проаналізовано організаційно-технічні методи обмеження доступу до серверу.

Організаційні заходи захисту інформації - комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціювання засобів забезпечення ІД та засобів забезпечення ТЗІ. Основні організаційні заходи: створення відповідального підрозділу якому надаються повноваження щодо організації й впровадження технології захисту інформації, контролю стану захищеності інформації − СЗІ; сервер, що здійснює зберігання та обробку конфіденційної інформації, повинен розташовуватися в приміщенні, доступ до якого обслуговуючого персоналу та користувачів різних категорій здійснюється в порядку, що визначений СЗІ та затверджений керівником установи (організації);

Для захисту інформації на рівні апаратного забезпечення використовуються:апаратні ключі; системи сигналізації. Для захисту периметра інформаційної системи створюються:системи охоронної й пожежної сигналізації; системи цифрового відеоспостереження; системи контролю й керування доступом (СККД). Захист інформації від її витоку технічними каналами зв’язку забезпечується наступними засобами й заходами: використанням екранованого кабелю й прокладкою проводів і кабелів в екранованих конструкціях; установкою на лініях зв’язку високочастотних фільтрівпобудовою екранованого приміщення для серверу.

ЧЕРВЬ – СЕТЕВОЙ ВИРУС

Степанов В. А.
Харьковский национальный университет радиоэлектроники, Харьков

Сетевые вирусы – это чрезвычайная опасность со стороны локальных сетей и Интернета включительно. Вирусы, проникая на компьютер через сеть, могут привести не только к повреждению важной информации, но и самой системы в целом.

Сетевых вирусов множество, одним из известных вирусов является сетевой червь.

Червь (сетевой червь) – тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных систем, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, осуществлению иного вредоносного воздействия. Зачастую черви даже безо всякой полезной нагрузки перегружают и временно выводят из строя сети только за счёт интенсивного распространения. Типичная осмысленная полезная нагрузка может заключаться в порче файлов на компьютере-жертве (в том числе, изменение веб-страниц, «deface»), заранее запрограммированной DoS-атаке с компьютеров жертв на отдельный веб-сервер, или бэкдор для удалённого контроля над компьютером-жертвой. Часто встречаются случаи, когда новый вирус эксплуатирует бэкдоры, оставленные старым.

В современном мире нельзя игнорировать вопросы информационной безопасности. В ответ на новые угрозы нужно искать новых подходы к реализации стратегии защиты информации и использовать новые методы и средства обеспечения сетевой безопасности.

ROOTKIT – ОДИН ИЗ ОСНОВНЫХ СЕТЕВЫХ АТАК

Ушатов В.В.
Харьковский национальный университет радиоэлектроники, Харьков

«Сетевые атаки» – сегодня это словосочетание знакомо любому пользователю компьютера. Многие уже успели стать жертвами злоумышленников. Говоря об угрозах в информационной сфере, мы не можем избежать хотя бы краткого описания типов сетевых атак. Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Одной из таких атак является Rootkit.

Rootkit – программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе. Большинство из реализаций современных rootkit могут прятать от пользователя файлы, папки и ключи реестра, скрывать запущенные программы, системные службы, драйверы и сетевые соединения. Т.е. злоумышленник имеет возможность создавать файлы и ключи реестра, запускать программы, работать с сетью и эта активность не будет обнаружена администратором. Кроме того, rootkits могут скрывать сетевую активность путем модификации стека протоколов TCP/IP. Так, например rootkit Hacker Defender перехватывает вызовы Winsock и может обрабатывать сетевой трафик до того как он будет передан приложению. Т.е. если в системе установлен Web сервер, и соответственно открыт 80-й порт, rootkit может использовать его для взаимодействия с взломщиком, в то время как другие пользователи будут без проблем работать по протоколу HTTP.

Важно понять, что сетевая безопасность - это эволюционный процесс. Нет ни одного продукта, способного предоставить корпорации «полную безопасность».

ARP-СПУФИНГ, КАК МЕТОД ПЕРЕХВАТА ТРАФФИКА

Бондарь Д.В.
Харьковский национальный университет радиоэлектроники, Харьков

В данный момент протокол ARP повсеместно используется во всех небольших офисных, публичных и пользовательских локальных сетях Ethernet. Так как ARP имеет ряд недостатков и уязвимостей это позволяет производить атаку на данный сетевой протокол именуемой как ARP-spoofing (ARP – poisoning).

ARP-spoofing происходит, когда злоумышленник, находящийся внутри сети выдает себя за ложное вычислительное устройство (роутер, маршрутизатор, шлюз). Суть атаки заключается в перехвате широковещательного ARP запроса и отправке ложного ARP – ответа в котором злоумышленник объявляет себя узлом связи(маршрутизатор). Данное действие меняет таблицу маршрутизации выбранного устройства и позволяет заинтересованному лицу контролировать сетевой траффик дезинформированного узла пропуская траффик через собственное устройство. Вышеперечисленные действия дают возможность перехватывая пакеты, которые могут содержать важные для пользователя данные: логины и пароли, передаваемые по незащищенному протоколу http, cookie файлы, которые содержат сессии на многих веб сайтах (социальные сети, интернет-магазины, онлайн-банкинг и т.д.). Некоторые программные пакеты, для организации данных атак, позволяют получать доступ к изображениям, которые пользователь просматривает в сети Интернет, подменять сайты и производить любые манипуляции над траффиком вплоть до возможности предоставления доступа к устройству с использованием других атак и уязвимостей.

Данная атака является одним из видов MITM (Man in the middle) атак базирующейся на недостатке протокола ARP. Он не проверяет подлинность ARP-запросов и ARP-ответов тем самым позволяя подменять их. Единственным решением для предотвращения атаки APR-spoofing, как и любой атаки “man in the middle” является использование шифрования пакетов, а именно использование протокола IPSec или PPPoE.

ТЕХНОЛОГІЇ КЕРУВАННЯ ДОСТУПОМ ТА МЕТОДИ АВТЕНТИФІКАЦІЇ

В'юхін Д.О., Евгеньев А.М.
Харьковский национальный университет радиоэлектроники, Харьков

В роботі розглянуто та проаналізовано технології керування доступом, та особливості деяких методів.

Керування доступом, згідно НД ТЗІ, – це сукупність заходів з визначення повноважень і прав доступу, контролю за додержанням ПРД. Керування доступом використовується для забезпечення основних принципів безпеки, таких як: Цілісність, Доступність, Конфіденційність. Також невід'ємною частиною керування доступом є ідентифікація та автентифікація, тому що людина повинна спочатку пройти ідентифікацію або автентифікацію для отримання доступу до потрібної інформації. Існує три основні методи, які використовуються для автентифікації — «щось знати» (автентифікація по знанню), «щось мати» (автентифікація по володінню), «кимось бути» (автентифікація за характеристиками).

Існують багато методів керування доступом, у роботі було розглянути 4 таких методи:

1) Керування доступом на основі правил. Суть методу полягає в тому, використовує певні правила, які вказують на те, що суб'єкт може і що не може робити з об'єктом. Це засновано на простих правилах (типу, «якщо X - то Y»). Наприклад, якщо ідентифікатор користувача відповідає аналогічному ідентифікатором в пред'явленому їм цифровому сертифікаті, користувачеві дозволяється доступ.

2) Обмежений інтерфейс користувача. Обмежує можливості доступу користувачів до окремих функцій, інформації або окремим системних ресурсів. Наприклад користувач, у якого немає повноважень переглядати деякі файли, навіть не побачить їх.

3) Матриця контролю доступу. Таблиця суб'єктів і об'єктів, що містить інформацію про те, які дії конкретні суб'єкти можуть робити з конкретними об'єктами.

4) Списки контролю доступу. Це списки суб'єктів, яким дозволений доступ до певного об'єкту, із зазначенням рівня дозволеного доступу.

Проведений аналіз показав, що кожна компанія сама вирішує, який тип моделі управління доступом вона збирається використовувати, вона повинна визначити і вдосконалити свої техніки і технології для підтримки цієї моделі.

СИСТЕМА МОНИТОРИНГА ДАВЛЕНИЯ В АВТОМОБИЛЬНЫХ ШИНАХ

Мзоков В.Г., Желтухин А.В., доц. Галькевич А.А.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков

Данная система использует бесконтактный метод считывания с датчиков, которые имеют уникальное ID и позволяет использовать данные датчики в различных системах, таких как:

- автоматическое отслеживание проезжающих машин и поиск угнанных;
- использование в системе автоматической оплаты проезда по платным дорогам;
- автоматизация оплаты платной парковки;
- использование в системе пропускного режима для автотранспорта.
- задача состоит в том, чтобы повысить в системе уровень защиты идентификации автомобиля.
- это можно достигнуть, если ID-метка откликается на определённый запрос. Использование данной технологии:
- позволит автоматизировать контроль за оборотом транспортных средств;
- позволит автоматизировать идентификацию транспортного средства;
- повысит защиту окружающей среды от загрязнения.

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

АНАЛІЗ НОРМАТИВНО-ПРАВОВИХ ДОКУМЕНТІВ ЩОДО ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Труш В. Є.
Харьковский национальный университет радиоэлектроники, Харьков

Політика інформаційної безпеки є однією із основних компонентів комплексної системи захисту інформації, і тому залишається актуальною для досліджень, як необхідна частина фундаменту для створення системи захисту інформації.

Метою дослідження є аналіз нормативно-правової бази України, порівняння тлумачення терміну «політика безпеки» та розгляд основних документів, які регламентують політику інформаційної безпеки в організації.

Згідно з НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» – політикою інформаційної безпеки є набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз.

НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації в автоматизованій системі, зокрема й документів, які стосуються політики інформаційної безпеки.

Загалом, політика інформаційної безпеки, як правила обробки інформації, розробляється згідно з положеннями НД ТЗІ 1.1-002 та рекомендаціями НД ТЗІ 1.4-001. ЇЇ рекомендується оформляти у вигляді окремого документу – Плану захисту.

ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ В СТАРТАПАХ

Дмитриев К.И.
Национальный университет радиоэлектроники, Харьков

В докладе рассмотрены следующие моменты: наличие описанной и защищенной интеллектуальной собственности позволяет ей распоряжаться. В соглашении о использовании ее одним из пунктов значится четкое определения объектов и субъектов интеллектуальной собственности и прав собственности. Неформализованная идея не может быть передана таким образом третьим лицам, соответственно из не нельзя извлекать прибыль. Интеллектуальная собственность должна быть защищена на определенных ранках. Рынки должны быть описаны географически (защищать необходимо в каждой стране отдельно) и по сегментам. Рассмотрены основные способы защиты интеллектуальной собственности: паттерны, промышленные секреты, копирайт, защита торговой марки. Патент — это документ, выданный специальным органом страны, который определяет исключительное право, авторство и приоритет изобретения, или промышленного образца в течение определенного времени и на определенной территории. Промышленные секреты включают в себя комплект мероприятий: ограничение доступа к частям технологии, содержащей промышленные секреты, разработка политик по защите и разглашению, внимательная проверка людей, которых набираем на работу. При помощи копирайта может быть защищен исходных код системы, дизайн интерфейса, контент. Имущественные права — это права распоряжаться правом получения дохода от интеллектуальной собственности. Это право отчуждаемо. Если авторов несколько, то они все имеют одинаковые права на интеллектуальную собственность и могут ей распоряжаться независимо друг от друга. Именно поэтому почти всегда вместе с полученным патентом, авторы заключают соглашение в котором прописывают взаимные обязательства при распоряжении такой интеллектуальной собственностью. Именно на имущественном праве и строится технологический бизнес.

АКТУАЛЬНІ ПИТАННЯ ПІДГОТОВКИ ФАХІВЦІВ ПОВІТРЯНИХ СИЛ ЗБРОЙНИХ СИЛ УКРАЇНИ

Ільїна І.В., Шевяков Ю.І.
Харківський Національний університет Повітряних Сил,
ім. І.Кожедуба, Харків

Сучасний рівень автоматизації і комп'ютеризації систем управління, впровадження новітніх інформаційних технологій практично у всі сфери життя українського суспільства, у тому числі і у військову сферу, вдосконалення засобів зв'язку і обробки даних обумовлюють створення єдиного інформаційно-телекомунікаційного простору управління.

У епоху «інформаційної ери» XXI століття, на перше місце виходять нові інформаційні технології, які, на думку ряду зарубіжних експертів, дозволять на практиці реалізувати «революцію» у військовій справі. Їх впровадження у військову сферу направлене на підвищення бойових можливостей формувань і ефективності військового управління, в першу чергу, за рахунок забезпечення всіх учасників бойових дій своєчасними і точними даними ситуаційної обізнаності щодо обстановки на полі бою, скорочення циклу бойового управління, а також автоматизацію проце-сів інформаційного, технічного і тилового забезпечення підрозділів.

Загальнодоступність і висока оперативність оновлення інформації про бойову обстановку, у поєднанні з її наочністю і високою достовірністю «єдиної цифрової картини поля бою», перетворюють інформацію на могутню зброю, без якою вже не представляється можливим ведення бойових дій.

Метою доповіді є висвітлення результатів аналізу рівня автоматизації і комп'ютеризації систем управління в Повітряних Силах ЗС України.

Запропоновано комплекс науково-методичних, організаційних, та інженерно-технічних заходів, щодо підвищення якості підготовки фахівців освітньо-кваліфікаційного рівня бакалавр, магістр для Збройних Сил України.

ДОСЛІДЖЕННЯ НОРМАТИВНИХ ДОКУМЕНТІВ ЩОДО РИЗИКІВ КІБЕРБЕЗПЕКИ МЕДИЧНИХ ПРИСТРОЇВ

Жиденко М.А., Стрєлкіна А.А.
Національний аерокосмічний університет ім. Н.Є. Жуковського «ХАІ», Харків

В доповіді представлені результати дослідження можливих вразливостей медичних систем на основі Інтернету речей. Розглянуті основні стандарти, що регулюють норми для забезпечення безпеки медичних пристроїв та комп'ютерних мереж у лікарнях (від організацій FDA та HIPAA). Запропоновані документи наголошують на важливості оцінювання ймовірностей виникнення загроз і зменшення наслідків до їх можливого виникнення.

Медичні системи для повного контролю за станом пацієнтів складаються з безлічі пристроїв з різноманітною функціональністю та рівнем захищеності. FDA пропонує класифікацію цих пристроїв для того, щоб визначити рівень захищеності кожної складової системи та провести необхідні дії до впровадження всіх складових:

– безпечні (I клас), що не потребують дозволу на використання;
– з певним ризиком (II клас), що потребують проведення дослідження;
– небезпечні (III клас), які необхідно перевіряти за допомогою випробування та багаторазової експертизи.

Кожен виробник повинен захистити свій пристрій незалежно від класифікації. Якщо це не можливо провести, то слід дотримуватись норм, що приводить HIPAA. У нормативних документах FDA приведені рекомендації щодо впровадження комплексних програм ризик-менеджменту до реалізації системи чи окремого приладу. Основні складові такого методу полягають у вмінні чітко виявляти та оцінювати загрози, впровадженні систем зменшення наслідків про виникненні ризику, прийнятті узгодженої політики та практики виявлення вразливостей та відстеженні інформаційних джерел у сфері кібербезпеки з метою виявлення можливих ризиків та загроз.

Проведений аналіз діючих документів показав, що для максимального забезпечення безпеки медичних пристроїв необхідно дотримуватись стандартів у комплексі, не обмежуючись лише одним.

ПРОБЛЕМИ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Петрук В.В.
Харківський національний університет радіоелектроніки, м.Харків

У доповіді розглянуто найважливіші проблемі міжнародного регулювання інформаційної безпеки та запропоновані деякі способи вирішення цих проблем. Прогрес в інформаційно-технологічній сфері поряд з об'єктивними благами, створив принципово нові потенційні загрози використання досягнень з цілями несумісними із завданнями підтримки миру та безпеки.

Усвідомлення необхідності дотримання принципів міжнарод- ного права, забезпечення прав і свобод, невикористання інформаційно-комунікаційних технологій з протиправною метою, – все це привернуло увагу до розгляду проблем міжнародно-правового ре- гулювання інформаційної безпеки, у тому числі і як підстави для обмеження інформаційних прав людини.

Інформаційна безпека – це стан захищеності встановлених за- конодавством норм та параметрів інформаційних процесів та відно- син. Причини виникнення інформаційної небезпеки можуть бути різними, але у всіх випадках вони зв'язані з природою інформації, її сутністю і роллю в життєзабезпеченні соціальних систем.

Стурбованість виникає перш за все у зв'язку з можливістю використання колосального потенціалу інформаційних кіберне- тичних технологій в інтересах забезпечення військово-політичної переваги, силового протистояння, шантажу, тим самим відкриваючи нові напрямки гонки озброєнь.

Проблеми заборони розробки і використання інформаційної зброї і, як наслідок, інформаційної війни навряд можуть бути ви- значені лише на міждержавному рівні. Значної уваги цим питанням приділяють міжнародні організації (ООН, ЄС, СНД, ШОС, ОЕСР), які на сьогодні зосередилися на пошуку загальних підходів до вирішення правових проблем міжнародної інформаційної безпеки.

ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В АЭРОКОСМИЧЕСКОЙ И ОБОРОННОЙ ПРОМЫШЛЕННОСТИ

Потякова К.О.
Харьковский национальный университет радиоэлектроники, Харьков

Похищения интеллектуальной собственности является одним из самых больших и потенциально опасных рисков для современной авиастроительной компании. Это риск, к которому большинство компаний очень слабо подготовлено. Когда речь заходит о защите интеллектуальной собственности в авиакосмической и оборонной промышленности, генеральным подрядчикам приходится сталкиваться с особыми рисками. Необходимость сокращения времени и затрат на создание сложных изделий, таких как самолеты и системы вооружения, вынуждает компании отдавать все больше ответственности за разработку и интеграцию основных подсистем своим подрядчикам. При этом подрядчики получают доступ к ценным данным, которые никак не должны попасть в руки конкурентов. А одним из главных приоритетов для компаний аэрокосмической и оборонной промышленности являются соображения национальной безопасности и, соответственно, защиты информации. Современный подход сосредотачивается вокруг развертывания нового поколения систем управления жизненным циклом изделия (PLM). PLM-платформа позволяет объединить данные из нескольких систем управления и создать центральное хранилище информации по всем проектам. Таким образом, PLM-платформа выполняет задачу по контролю за разработкой продукции и защиты интеллектуальной собственности. При применении PLM-решений все запросы на доступ к интеллектуальной собственности в рамках любого проекта управляются единой системой, способной в реальном времени определить право доступа пользователя к запрашиваемой информации, исходя из его полномочий и физического местоположения. PLM-системы обеспечивают не только полный контроль и простое управление всей информацией о технологических процессах, связанных с проектированием, разработкой и обслуживанием изделий, но также и надежно защищают всю информацию о производственном процессе. Они применяются в оборонной и аэрокосмической отрасли многих стран мира.

ОБЕСПЕЧЕНИЕ ПРАВОВОЙ КИБЕРБЕЗОПАСНОСТИ ИГРОВЫХ ДВИЖКОВ

Руденко В.О.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков

Одним из наиболее сложных объектов авторского права является компьютерная программа. В данном объекте интеллектуальной собственности тесно переплетены программный код, который рассматривается законами Украины как литературное произведение и наличие в программе алгоритмов исполнения кода, которые ближе к патентному праву, где алгоритм сродни изобретению.

Игровой движок – это инструмент, созданный для упрощения и ускорения разработки игр и предоставляет возможность запуска игр на нескольких платформах. Игровые движки по типам лицензий делятся на четыре категории. Внутренние, используются только в собственных проектах и не продаются сторонним лицам, примером является 4A Engine разработанной украинской компанией «4A Games» для использования в компьютерной игре «Metro 2033». Коммерческие, создаются с целью получения прибыли от их использования, примером является популярный физический движок Havok, разработанный ирландской компанией «Havok». Проприетарные – частная собственность авторов не удовлетворяющая критериям свободного программного обеспечения, примером является «Anvil Engine» созданный дочерней студией «Ubisoft Montreal» и впервые использованный в «Assassin's creed». Свободные – предоставляют пользователю право на установку, использование, изучение, изменения и распространение, примерами являются Irrlicht Engine и Cocos2d.

Лучшим выбором для «одиночной» разработки является свободная лицензия, она предоставляет возможность продемонстрировать продукт без затрат на рекламную кампанию, а так же выбрать один из вариантов лицензии – с возможностью изменения программного продукта, но с запретом назвать результат оригинальным, и без возможности изменения, позволяющая использовать код только в закрытом программном обеспечении.

ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Щипанов М.В.
Национальный технический университет «ХПИ», Харьков

Суть правовой защиты компьютерной информации. Цели правовой защиты конфиденциальной информации. Политика обеспечения защиты информации. Проблемы, влияющие на проведение этой политики в жизнь. Угрозы конфиденциальности информации. Ответственность за несанкционированный доступ к информации, которая составляет служебную или коммерческую тайну, незаконное получение в свое распоряжение и распространение информации, нормативно-правовые акты, которыми она предусмотрена. Конституционное законодательство в сфере компьютерной информации, общие законы, кодексы. законы об организации управления, специальные законы, подзаконные нормативные акты по защите информации. Необходимость усовершенствования комплекса мер по правовой защите системной информации. Страховое обеспечение защиты информации, цели страхования. Лицензирование. Контроль за соблюдением неразглашения конфиденциальной информации пользователями, осуществляемый за счет надежной защиты конфиденциальной информации при подключении организации к сети Интернет. Эффективное управление доступом пользователей и предотвращение НСД к важным сведениям, в том числе при использовании технологии виртуализации. Защита автоматизированных рабочих мест и серверов от широкого спектра внешних и внутренних угроз. Криптографическая защита информации при передаче по каналам связи между удаленными офисами и при взаимодействии с сотрудниками, работающими вне офиса. Необходимость оповещения сотрудников о секретной информации и санкциях за её разглашение. Закон об информации. Интеллектуальная собственность и авторское право. Служебная и профессиональная тайна. Оценка эффективности принимаемых мер защиты информации. Источники правового регулирования конфиденциальной информации как условия трудового договора. Требования информационной безопасности и ограничения для них. Преступления в сфере компьютерной информации. Неправомерный доступ к компьютерной информации. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей Создание, использование и распространение вредоносных компьютерных программ.

АНАЛІЗ ЯКОСТІ ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ІНФОРМАЦІЙНОЇ СИСТЕМИ СУДОВОЇ ЕКСПЕРТИЗИ

Можаєв[1] О.О., Можаєв[2] М.О., Логвиненко[2] М.О.
[1]Национальный технический университет «ХПИ», Харьков
[2]Харківський НДІ судових експертиз

Різноманітна за формами і змістом судово-експертна діяльність неможлива без залучення інформаційних ресурсів, під якими законодавець розуміє окремі документи і окремі масиви документів, документи і масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, інших інформаційних системах). Інформаційне забезпечення судової експертизи має являти собою інформаційний процес, який визначається законодавцем як процес збору, обробки, накопичення, зберігання, пошуку і розповсюдження інформації, необхідної в даному випадку для вирішення судово-експертних завдань.

Для обміну інформацією в інформаційних системах судово-експертної діяльності використовуються як локальні комп'ютерні мережі, наприклад, при здійсненні криміналістичної реєстрації, так і глобальна мережа Інтернет. Це примушує користувачів ставити питання про ефективність систем контролю, захисту та передачі інформації. Через велике зростання інформації, навантаження на комп'ютерну мережу істотно збільшується.

Завдання управління процесом передачі даних продиктована необхідністю підтримувати в мережі трафік необхідного обсягу з певними вимогами якості обслуговування. Коли необхідний розмір смуги пропускання з'єднання перевищує доступний, може проявитися перевантаження. Можливими причинами, які породжують перевантаження, є наступні: високошвидкісні сполуки з великим часом передачі пакетів; тимчасові перевантаження; неоптимальні топології та неузгоджені швидкості каналів; протоколи, несуттєво знижують швидкість відправки пакетів в мережу при виникненні перевантаження.

В результаті проведених теоретичних досліджень і імітаційного моделювання встановлено, що пропонована система оцінки параметрів мережі інформаційної системи судово-експертної діяльності дозволяє визначати місце розташування ділянок телекомунікаційної мережі з обмеженою пропускною спроможністю.

СОЗДАНИЕ ГЕОИНФОРМАЦИОННОЙ СИСТЕМЫ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА ИРАКА

Можаев А.А., Наем Хазим Рахим
Национальный технический университет «ХПИ», Харьков

Современная экологическая ситуация в Ираке характеризуется нарастанием симптомов экологической катастрофы. В этих условиях проблемы охраны окружающей среды и рационального природопользования становятся чрезвычайно важными. В Ираке отсутствуют какие-либо структурированные системы управления охраной окружающей среды на предприятиях, которые гарантировали бы при достижении финансово-экономических целей экологическую безопасность. Причина кроется в глубоком несовершенстве существующей экологической политики в стране. Целью данного исследования является анализ существующих геоинформационных систем (ГИС) и определение перспектив создания и внедрения ГИС экологического мониторинга в Ираке.

Мониторинг включает три основных направления деятельности:

наблюдения за факторами воздействия и состоянием среды;

оценку фактического состояния среды;

прогноз состояния окружающей природной среды и оценку прогнозируемого состояния.

Для Ирака основными задачами экологического мониторинга можно считать:

1. Исследование почв, ветряных эрозий, песчаных бурь.

2 Исследование стоков рек (горных), наводнения.

3 Мониторинг состояния нефте-, газо месторождений, нефте-, газо проводов и танкерных терминалов

4 Сравнение использования для ГИС спутниковых систем мониторинга, систем мониторинга, установленных на самолетах, беспилотниках, а также средства мониторинга наземного базирования

ГИС экологического мониторинга, реализующая задачи экологической и техногенной безопасности региона, должна базироваться на сетевой управляющей вычислительной системе (УВС), построенной с применением эффективных программных и технических средств. УВС экологической и техногенной безопасности региона можно представить как сетевой комплекс, объединяющий измерительные устройства и контроллеры пунктов мониторинга, рабочие станции центра мониторинга между собой, а также с уровнем управления регионом.

ОРГАНІЗАЦІЙНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Дерев'янко О.О.
Харківський національний університет радіоелектроніки, Харків

Одними з першочергових заходів на шляху побудови системи кібербезпеки держави є вдосконалення державного управління у цій сфері та створення нормативно-правової бази для забезпечення цієї діяльності. З метою забезпечення кібербезпеки України має бути створено національну систему кібернетичної безпеки як формат співробітництва державних органів, установ, організацій, приватного сектору економіки, наукових установ і організацій, професійних асоціацій та неурядових організацій у сфері кібербезпеки. Основою національної системи кібернетичної безпеки є державні органи, які відповідно до покладених завдань безпосередньо виконують функції щодо забезпечення безпеки кіберпростору України. До участі у здійсненні заходів, пов'язаних із виявленням, запобіганням і нейтралізацією кібернетичних загроз, залучаються інші суб'єкти забезпечення кібернетичної безпеки. Координація діяльності всіх суб'єктів забезпечення кібернетичної безпеки повинна здійснюватись Радою національної безпеки і оборони України через її робочий орган – Інформаційно-аналітичний центр, який відповідає за забезпечення аналітичного та прогнозного супроводження діяльності РНБО України з питань національної безпеки в інформаційній сфері.

ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кравчук П.В.
Харьковский национальный университет радиоэлектроники, Харьков

Отечественный ИТ-рынок в последние несколько лет динамично развивается. По оценкам экспертов его рост превышает 10% в год. При этом сектор информационной безопасности (ИБ) развивается еще более быстрыми темпами – более чем на 25% в год. Такой рост определяется в основном двумя факторами: возросшим вниманием руководства к обеспечению ИБ и недостаточным уровнем ИБ в существующих информационных системах (ИС).

Уже сейчас в отечественных ИС с повышенными требованиями в области ИБ (банковские системы, ответственные производства, и т.д.) затраты на обеспечение режима ИБ составляют до 30% всех затрат на ИС, и владельцы информационных ресурсов серьезно рассматривают экономические аспекты обеспечения ИБ. Начальники служб автоматизации, исполнительные директора, начальники служб информационной безопасности должны иметь понятные для бизнеса аргументы для обоснования инвестиций в ИБ, т.е., по сути, представлять обоснование стоимости системы ИБ для бизнеса.

В обосновании затрат на ИБ существует два основных подхода. Первый подход, назовем его наукообразным, заключается в том, чтобы освоить, а затем и применить на практике необходимый инструментарий измерения уровня ИБ. Для этого необходимо привлечь руководство компании к оценке стоимости информационных ресурсов, определению оценки потенциального ущерба от нарушений в области ИБ. От результатов этих оценок будет во многом зависеть дальнейшая деятельность руководителей в области ИБ. Второй подход состоит в следующем: можно попытаться найти инвариант разумной стоимости корпоративной системы защиты информации.

Реализация этих подходов (конкретные методы оценки эффективности системы ИБ) на практике зависит от ряда факторов, среди которых основными являются степень зрелости организации и специфика ее деятельности, поэтому выбор соответствующего метода является очень важным решением в обеспечении ИБ.

УЧАСНИКИ КОНФЕРЕНЦІЇ:

ЗМІСТ

ПЛЕНАРНЕ ЗАСІДАННЯ

СЕКЦІЯ 1
ПРОБЛЕМИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ \ ТА ПРОГНОЗУВАННЯ ЗАГРОЗ КІБЕРБЕЗПЕКИ

СЕКЦІЯ 2
ОРГАНІЗАЦІЙНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

СЕКЦИЯ 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 другої міжнародної науково-практичної конференції (10 квітня – 12 квітня 2017 року)

Відповідальна за випуск *Т. М. Шипова*
Технічний редактор *Г. В. Гейко*
Коректор *С. С. Бульба*
Комп'ютерне складання та верстання *Т. М. Шипова*

Формат 60 × 84/16. Ум.-вид. арк. 6,51. Тираж 200 пр. Зам. 404-17

Адреса оргкомітету: вул.. Кирпичова, 2, м. Харків, 61002, Україна
Національний технічний університет «Харківський політехнічний інститут»
Тел. **(057) 707-61-65**

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: **bookfabrik@rambler.ru**