4 Реферати

УДК 004.056.5

АНАЛИЗ УГРОЗ И УЯЗВИМОСТЕЙ ИНДУСТРИАЛЬНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Сергей Гончар, Геннадий Леоненко, Алексей Юдин
ГосНИИ Спецсвязи

Стаття: ***6 стор. 3 джерела***

В настоящее время индустриальные автоматизированные системы управления (ИАСУ), которые включают системы диспетчерского управления и сбора данных (SCADA), системы распределенного управления и другие конфигурации систем управления, используются в отраслях, которые жизненно важны для инфраструктуры государства. И если изначально ИАСУ были в виде отдельных компьютеров с собственными операционными системами и сетями, то на сегодняшний день происходит их интеграция с корпоративными системами и другими бизнес-приложениями через различные системы связи, включая Интернет.

Процесс интеграции позволяет обеспечивать управление производственной деятельностью в режиме реального времени, осуществлять дистанционный мониторинг систем управления технологическим процессом, повысить безопасность предприятия и персонала, снизить расходы на эксплуатацию. Однако ценой этих преимуществ является постоянно растущая уязвимость к угрозам.

Угрозы для ИАСУ могут исходить из различных источников: умышленных (террористические группы, промышленные шпионы, недовольные сотрудники, злоумышленники), непреднамеренных (сложность системы, человеческие ошибки, аварии, отказы оборудования), природных (стихийные бедствия, климатические условия и т. п.).

Уязвимостью является недостаток или слабое место информационной системы, системы безопасности, процедур внутреннего контроля, которые могут быть использованы для нарушения целостности или доступности системы и ее корректной работы. Анализ уязвимостей индустриальных автоматизированных систем управления дает возможность провести их структуризацию по трем категориям: уязвимости политик и процедур, уязвимости программных платформ ИАСУ, уязвимости сетей.

Уязвимости политик и процедур в ИАСУ возникают из-за отсутствия или неполной, неадекватной документации в области безопасности, в том числе политик и руководства по внедрению (процедур), администрированию аудиту, восстановлению.

Уязвимости программнылатформ в ИАСУ могут возникать из-за недостатков, ошибок, или некачественного обслуживания своих платформ, в том числе оборудования (аппаратных средств), операционных систем и приложений, отсутствие контроля физического доступа.

Уязвимости сети в ИАСУ могут возникать из-за недостатков, ошибок, или плохого администрирования сетей ИАСУ и их соединений с другими сетями. Эти уязвимости могут быть устранены или нивелированы с помощью правильного проектирования сети, шифрования сетевых соединений, обеспечения контроля физического доступа к сетевым компонентам.

Проведенный анализ угроз и уязвимостей ИАСУ дает представление о возможных рисках для данных систем, позволяет сформулировать некоторые требования и ограничения по применению возможных мер, методов и средств защиты информации при создании комплексных систем защиты информации.

АНАЛІЗ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ ІНДУСТРІАЛЬНИХ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ

Сергій Гончар, Геннадій Леоненко, Олексій Юдін
ДержНДІ Спецзв'язку

Наразі індустріальні автоматизовані системи управління (ІАСУ), які складаються з систем диспетчерського управління та збору даних (SCADA), систем розподіленого управління та інших конфігурацій систем управління, використовуються в галузях, які є життєво важливими для інфраструктури держави. І якщо первісно ІАСУ існували у вигляді окремих комп'ютерів з власними операційними системами та мережами, то на сьогодні відбувається їх

інтеграція з корпоративними системами і іншими бізнес-прикладними програмами через різні системи зв'язку, включаючи Інтернет.

Процес інтеграції дозволяє забезпечувати управління виробничою діяльністю в режимі реального часу, здійснювати дистанційний моніторинг систем управління технологічним процесом, підвищувати безпеку підприємства та персоналу, знижувати витрати на експлуатацію. Проте, ціною цих переваг є постійно зростаюча вразливість до реалізації загроз.

Загрози для ІАСУ можуть виходити з різних джерел: навмисних (терористичні групи, промислові шпигуни, незадоволені співробітники, зловмисники), ненавмисних (складність системи, людські помилки, аварії, відмови обладнання), природних (стихійні лиха, кліматичні умови і т.ін.).

Вразливістю є недолік або слабке місце інформаційної системи, системи безпеки, процедур внутрішнього контролю, які можуть бути використані для порушення цілісності або доступності системи і її коректної роботи. Аналіз вразливостей індустріальних автоматизованих систем управління дає можливість провести їх структуризацію за трьома категоріями: вразливості політик і процедур, вразливості програмних платформ ІАСУ, вразливості мереж.

Вразливості політик та процедур в ІАСУ виникають через відсутність або неповну, неадекватну документацію в галузі безпеки, в тому числі політик і керівництв по впровадженню (процедур), адмініструванню аудиту, відновленню.

Вразливості програмних платформ в ІАСУ можуть виникати через недоліки, помилки, або неякісне обслуговування платформ, в тому числі обладнання (апаратних засобів), операційних систем і прикладних програм, відсутності контролю фізичного доступу.

Вразливості мережі в ІАСУ можуть виникати через недоліки, помилки або погане адміністрування мереж ІАСУ та їх з'єднань з іншими мережами. Ці вразливості можуть бути усунені або нівельовані за допомогою правильного проектування мережі, шифрування мережевих протоколів, забезпечення контролю фізичного доступу до мережевих компонентів.

Проведений аналіз загроз та вразливостей ІАСУ дає уяву про можливі ризики для цих систем, дозволяє сформулювати деякі вимоги та обмеження щодо застосування можливих заходів, методів та засобів захисту інформації при створенні комплексних систем захисту інформації.

THE ANALYSIS OF THREATS AND VULNERABILITIES OF THE INDUSTRIAL AUTOMATED CONTROL SYSTEMS

Sergii Gonchar, Gennady Leonenko, Oleksii Yudin
SRI for STIP

Now the industrial automated management systems (IAMS) which include supervisory control system and data acquisition (SCADA), systems of the distributed control and other configurations of management systems are used in the branches, which vital states for an infrastructure. Moreover, if originally IAMS were in the form of separate computers with characteristic operating systems and webs for today there is their integration to enterprise systems and other business applications through various communications systems, including the Internet.

Integration process allows ensuring control of industrial activity real time, to carry out remote monitoring of management systems by a technological process, to raise safety of the factory and staff, to cut expenditures on maintenance. However by these advantages permanently growing vulnerability to threats is.

Threats for IAMS can start with various sources: deliberate (terrorist groups, the industrial spies, dissatisfied employees, malefactors), inadvertent (system complexity, human errors, crashes, hardware failures), natural (acts of nature, environmental conditions etc.).

Vulnerability are deficiencies or a feeble place of an information system, security arrangement, procedures of interior control that can be used for violation of integrity or accessibility of system and its correct operation. The analysis of vulnerabilities of the industrial automated management systems gives the chance to lead their structuration on three classes: vulnerability of policies and procedures, vulnerability of program platforms IAMS, vulnerability of webs.

Vulnerability of policies and procedures in IAMS originate because of lack or the incomplete, inadequate documentation in the field of safety, including policies and an administration on implementation (procedures), administration to audit, recovery.

Vulnerability of program platforms in IAMS can originate because of deficiencies, errors, or poor-quality service of the platforms, including the equipment (hardware), operating systems and applications, lack of control of physical access.

Vulnerability of a net in IAMS can originate because of deficiencies, errors, or the bad administration of nets IAMS and their joints with other nets. These vulnerabilities can be eliminated by means of the correct designing of a net, encryption of network connections, and control of physical access to network components.

The carried out analysis of threats and vulnerabilities of IAMS provides guidance on possible marks for the given systems, allows formulating some demands and restrictions on application of possible measures, methods and information security facilities at creation of complex systems of protection of the information.

УДК 681.3.06

МЕТОДИКА ФОРМУВАННЯ МНОЖИНИ ПОКАЗНИКІВ ЯК СКЛАДОВА МЕТОДУ ОЦІНЮВАННЯ РІВНЯ КУЛЬТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Олександр Потій, Дмитро Пилипенко*

*Харківський університет Повітряних Сил ім. І. Кожедуба, *Харківський національний університет раліоелектроніки*

Стаття: ***7 стор., 11 джерел.***

Розуміння питань управління процесами та діяльністю із захисту інформації (ЗІ) сьогодні зазнає якісних змін. Багато вчених та практиків поділяють наступну думку: організаційні аспекти ЗІ потребують не меншої уваги, ніж технічні. Про це також свідчать останні аналітичні звіти (InfoWatch), з яких стає зрозумілим, що більшість фінансових втрат відбувається через інциденти безпеки, пов'язані із витоком даних. При цьому організації страждають від дій власних співробітників в тій самій мірі, що й від дій зловмисників. Такі інциденти не завжди пов'язані з нестачею або неадекватністю процедур та практик захисту. Причина частіше полягає у недотриманні заходів захисту через хибне розуміння цілей та задач захисту. Сприйняття політики безпеки (ПБ) як обмеження та незручності призводить до формування низького рівня культури інформаційної безпеки (КІБ). Тут під «культурою інформаційної безпеки» розумітимемо набір норм, цінностей та настанов, що формують припустиму поведінку у контексті діяльності із захисту інформації.

Носіями КІБ виступають всі члени організації, а сама КІБ залежить від їхньої поведінки і діяльності, що дозволяє говорити про те, що питання формування КІБ пов'язані з управлінням нормами та обмеженнями. У контексті інституціонального управління КІБ слід розглядати в першу чергу як механізм спонукання, у той час як ПБ є механізмом змушення. Вибір керуючих впливів керівним суб'єктом не повинен спиратися лише на суб'єктивні фактори (досвід, знання, інтуїцію), оскільки більш обґрунтовані рішення можуть бути сформовані за допомогою показників безпеки. Таким чином, метою даної роботи є представлення методики формування множини показників оцінювання рівня КІБ, яку слід розглядати в контексті методу оцінювання рівня КІБ.

Стислий опис дозволить сформувати загальну уяву про розроблений метод оцінювання рівня КІБ і про те, яке місце посідає в ньому запропонована методика:

- на першому етапі формується множина показників оцінювання КІБ;
- на другому етапі розробляється шаблон показника оцінки КІБ нижнього рівня;
- на третьому етапі здійснюється побудова дихотомічного дерева комплексного оцінювання;
- на четвертому етапі здійснюється опис показників нижнього рівня згідно з шаблоном;
- на п'ятому етапі визначається розмірність и тип шкали оцінювання рівня КІБ;
- на шостому етапі здійснюється генерація матриць згортання з урахуванням вагових коефіцієнтів та мінімальних порогових значень, що визначаються експертом;
- на сьомому етапі здійснюється згортання значень показників безпосередньо.

Спираючись на результати аналізу найбільш популярних систем показників безпеки (Vaughn-Hennig-Siraj, OCTAVE, CISWG, Erkan Kahraman, NIST) було сформульовано наступний висновок: незважаючи на те, що показники організаційного характеру присутні у тому чи іншому вигляді в кожній із проаналізованих систем, цілісної системи (набору) показників, що дозволили б кількісно або якісно оцінити рівень КІБ, на даний момент не існує. Таким чином, виникає задача сформувати цілісну множину показників, що дозволяють здійснити комплексне оцінювання рівня КІБ. В результаті аналізу існуючих систем показників безпеки було сформовано базову множину показників, елементи якої було уточнено та узагальнено. Спираючись на онтологічну модель предметної галузі КІБ було розроблено додаткову множину показників оцінювання КІБ, завдяки якому було охоплено аспекти КІБ, які не було враховано елементами базової

множини. Об'єднання цих множин дозволило отримати множину, що містить мінімально необхідну кількість показників для оцінювання рівня КІБ.

Таким чином, в роботі запропоновано методику формування множини показників оцінювання КІБ, що входить до складу методу оцінювання рівня КІБ. Використання вказаної методики дозволило отримати фінальну множину з 27 унікальних показників, що охоплюють усі основні аспекти КІБ. Проте слід зазначити, що отримана в результаті множина показників не є остаточно визначеною і може буті доповнена новими показниками.

МЕТОДИКА ФОРМИРОВАНИЯ МНОЖЕСТВА ПОКАЗАТЕЛЕЙ КАК СОСТАВЛЯЮЩАЯ МЕТОДА ОЦЕНКИ УРОВНЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Александр Потий, Дмитрий Пилипенко*

*Харьковский университет Воздушных Сил им. И.Кожедуба, *Харьковский национальный университет радиоэлектроники*

Понимание проблем управления процессами и деятельностью по защите информации (ЗИ) сегодня претерпевает значительные качественные изменения. Многие ученые, исследователи и практики выражают единое мнение о том, что организационные аспекты ЗИ требуют не меньшего внимания, чем технические. В поддержку данной точки зрения служат также последние аналитические ответы (InfoWatch), из которых видно, что основные финансовые потери по причине инцидентов безопасности связаны с утечкой данных. При этом организации страдают от действий собственных сотрудников в той же мере, как и от действий злоумышленников. Подобные инциденты не всегда связаны с нехваткой мер защиты или неадекватностью процедур и практик защиты. Причина чаще заключается в несоблюдении мер защиты и проистекает от неверного понимания целей и задач защиты. Восприятие политики безопасности (ПБ) как ограничения и неудобства приводит к формированию низкого уровня культуры информационной безопасности (КИБ). Здесь под «культурой информационной безопасности» будем понимать набор норм, ценностей и установок, которые формируют допустимое поведение в контексте деятельности по защите информации.

Носителями КИБ являются все члены организации, а сама КИБ зависит от их поведения и деятельности, поэтому можно говорить о том, что процесс формирования КИБ связан с управлением нормами и ограничениями. В контексте институционального управления КИБ следует рассматривать как механизм побуждения, в то время как ПБ является механизмом принуждения. Выбор управляющих воздействий руководящим субъектом не должен опираться исключительно на субъективные факторы (опыт, знания, интуицию), поскольку более обоснованные решения могут быть приняты на основе показателей безопасности. Таким образом, целью данной работы является представление методики формирования множества показателей оценки уровня КИБ, которую следует рассматривать в рамках метода оценки уровня КИБ.

Краткое описание позволит сформировать общее представление о разработанном методе оценки уровня КИБ и том, такое место занимает в нем методика формирования показателей оценки уровня КИБ:

- на первом этапе формируется множество показателей оценки КИБ;
- на втором этапе разрабатывается шаблон показателя оценки КИБ нижнего уровня;
- на третьем этапе осуществляется построение дихотомического дерева комплексной оценки;
- на четвертом этапе происходит описание показателей нижнего уровня;
- на пятом этапе определяется размерность и тип шкалы оценки уровня КИБ;
- на шестом этапе осуществляется генерация матриц свертки с учетом весовых коэффициентов и минимальных пороговых значений, которые определяются экспертно;
- на последнем, седьмом этапе осуществляется сама свертка значений показателей оценки КИБ.

На основании анализа наиболее популярных систем показателей безопасности (Vaughn-Hennig-Siraj, OCTAVE, CISWG, Erkan Kahraman, NIST) был сформулирован следующий вывод: несмотря на то, что показатели безопасности организационного характера присутствуют в том или ином виде в каждой из проанализированных систем, целостной системы (набора) показателей, позволяющей количественно или качественно оценить уровень КИБ, на данный момент не существует. Таким образом, возникает задача сформировать целостное множество показателей, позволяющих осуществить комплексную оценку уровня КИБ. В результате анализа существующих систем показателей безопасности было сформировано базовое

множество показателей, элементы которого были доработаны, уточнены и обобщены. Опираясь на онтологическую модель предметной области КИБ, было разработано дополнительное множество показателей оценки КИБ, благодаря которому были охвачены аспекты КИБ, не затронутые элементами базового множества. Объединение данных множеств позволило получить множество, содержащее минимально необходимое число показателей для оценки уровня КИБ.

Таким образом, в работе предложена методика формирования множества показателей оценки КИБ, которая является составляющей метода оценки уровня КИБ. На основании данной методики было получено итоговое множество показателей оценки КИБ, состоящее из 27 уникальных показателей, которые охватывают все ключевые аспекты КИБ. Однако следует заметить, что полученное итоговое множество показателей не является окончательно определенным и может быть дополнено новыми показателями.

AN APPROACH TO SET OF METRICS DEVELOPMENT AS A COMPONENT OF INFORMATION SECURITY CULTURE EVALUATION METHOD

Aleksandr Potii, Dmitry Pilipenko*

Kozhedub Air Force University, Kharkiv, *[2]Kharkiv national University of Radioelectronics

Current understanding of Information Security (IS) activities and processes management problems undergoes significant changes. Many researchers and specialists share the common concept that organizational aspects of IS are as important as technical ones. Latest analytical reports (InfoWatch) support this viewpoint, since major financial losses from security incidents relate to data loss. At the same time organizations suffer from their own personnel activities and behavior as bad as from adversaries. Such security incidents do not always occur due to lack or inadequacy of security controls and procedures. Noncompliance is usually the reason, which in its turn stems from poor understanding of security goals and objectives. Interpretation of Information Security Policy (ISP) as an obstacle or inconvenience results in low level of Information Security Culture (ISC). Here we interpret ISC as a set of norms, values and attitudes which create acceptable behavior in terms of IS activities.

Any organization member supports ISC which depends on their behavior and activities. Thus we can say that process of fostering ISC is connected with norms and limitations management. In terms of institutional management ISC can be interpreted as an incentive mechanism, while ISP is an enforcement mechanism. Control actions by top management should not be bases on subjective factors exclusively (experience, knowledge, intuition). More valid decisions can be made with the help of security metrics. The purpose of this paper is thus to propose an approach to development of ISC metrics set which should be considered within the method of ISC evaluation.

A brief description of method proposed is provided for general understanding, and more particularly about the place of mentioned above approach to ISC metrics development:

- in the first phase ISC metrics set is developed;
- in the second phase the template of ISC lower-level metric is designed;
- in the third phase the dichotomous tree for complex evaluation is build;
- in the fourth phase all lower-level metrics are described according to template;
- in the fifth phase dimension and type of scale for ISC evaluation is decided;
- in the sixth phase convolution matrices are generated with the help of weight coefficients and minimal thresholds estimated by experts;
- in the seventh phase the convolution of ISC metrics' values is done.

Analysis of the most popular security metrics systems (Vaughn-Hennig-Siraj, OCTAVE, CISWG, Erkan Kahraman, and NIST) allowed reaching the following conclusion: disregard the fact that security metrics of organizational type are present in each of chosen system; there is no holistic set of metrics which allows evaluating ISC level. The problem of developing such set of metrics is thus requires solving. Analysis of mentioned above security metrics systems allowed forming the basic set of ISC metrics, which was further adjusted. With the help of developed ontology model of ISC subject domain the set of ISC metrics was extended in order to cover all the key ISC features. The final set of ISC metrics represents the minimum quantity of metrics required for ISC evaluation.

An approach to development of ISC metrics set is proposed as a component of ISC evaluation method. Based on this approach the final set of 27 unique ISC metrics was developed. This is the minimum quantity of ISC metrics

required for comprehensive evaluation of organizational ISC. However, it should be noted that final set of ISC metrics is not a terminal set and can be extended with new metrics.

УДК 004.056:159.95

ТЕОРІЯ ІГОР ЯК МЕТОД УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Володимир Бурячок, Анатолій Шиян*
*Військова частина А1906, *Вінницький національний технічний університет*

Стаття: ***8 стор, 7 джерел.***

Управління інформаційною безпекою включає в себе управління людськими, інформаційними, технічними, програмними, фінансовими та іншими ресурсами. Людина, сукупність людей (як організована – підприємство, організація тощо, так і неорганізована – сукупність футбольних фанатів чи хакерів), суспільство і держава (та їх інститути) складають суб'єкти управління інформаційною безпекою. Метою статті є аналіз теорії ігор як кількісного методу, який суттєво розширює можливості при управлінні інформаційною безпекою, та визначення основних особливостей його застосування в даній предметні області. Наведено опис апарату теорії ігор та концепцій їх рішень. Виділено характеристики теорії ігор, які є перспективними для використання в методах управління інформаційною безпекою. Показано, що рівновага Неша є оптимальною для розв'язання багатьох задач з управління інформаційною безпекою. Як приклади застосування теорії ігор до задач управління інформаційною безпекою розглянуто: управління керівниками підприємства з боку його акціонерів; зменшення рівня ризиків при впровадженні другого рівня накопичувальної пенсійної системи; ризики для національної безпеки України, які виникають внаслідок взаємодії суб'єктів вітчизняної фінансової системи (окремих людей та структур) та фінансових систем розвинених країн. Проаналізовано розвиток теорії ігор в Україні та виявлено, що в країні відсутні спеціалісти, які здатні масово навчити студентів методам та технологіям діяльності, які використовуються в ринковій економіці. Відмічено, що наявність критичного стану інформаційної безпеки держави у предметній області економіки в Україні навіть не усвідомлюється.

ТЕОРИЯ ИГР КАК МЕТОД УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Владимир Бурячок, Анатолий Шиян*
*Военная часть А1906, *Винницкий национальный технический университет*

Управление информационной безопасностью включает в себя управление человеческими, информационными, техническими, программными, финансовыми и другими ресурсами. Человек, совокупность людей (как организованных – предприятие, организация и т.п., так и неорганизованных – совокупность футбольных фанатов или хакеров), общество и государство (и их институты) являют собой субъекты управления информационной безопасностью. Целью статьи является анализ теории игр как количественного метода, который существенно расширяет возможности при управлении информационной безопасностью и выявление основных особенностей ее применения данной предметной области. Приведено описание аппарата теории игр и концепций их решений. Выделены характеристики теории игр, которые являются перспективными для использования в методах управления информационной безопасностью. Показано, что равновесие Нэша является оптимальным для решения большинства задач управления информационной безопасностью. В качестве примеров применения теории игр к задачам управления информационной безопасностью рассмотрено: управления руководителями предприятия со стороны его акционеров; уменьшение уровня риска при внедрении второго уровня накопительной пенсионной системы; риски для национальной безопасности Украины, которые возникают вследствие взаимодействия субъектов отечественной финансовой системы (отдельных людей и структур) и финансовых систем развитых стран. Проанализировано развитие теории игр в Украине и обнаружено, что в стране отсутствуют специалисты, которые способны массово научить студентов методам та технологиям, которые применяются в рыночной экономике. Отмечено, что наличие критического состояния информационной безопасности государства в предметной области экономики в Украине даже не осознается.

GAME THEORY AS A METHOD OF INFORMATION SECURITY

Volodymir Buryachok, Anatoliy Shiyan*

*The military unit A1906,*Vinnitsa national technical university*

The information security management includes the management of human, information, technical, soft, financial and other resources. Man, a collection of people (organized - firm, organization, etc., and not organized - a set of football fans or hackers), society and the state (and their institutions) are the subjects of information security management. The paper analyzes the game theory as a quantitative method, which greatly enhances the information security management and identifies the main features of its application in given subject area. The description of the game theory and concepts of their decisions are described. The characteristics of game theory, which are promising for use in the methods of information security management, are marked. It is shown that the Nash equilibrium is optimal for most of the problems of information security management. As examples of the application of game theory to problems of information security management we considered: control managers of the enterprise from its shareholders; reduction of the level of risk in the implementation of the second-tier pension accumulation system; the risks to the national security of Ukraine, which arise from the interplay of the domestic financial system entities (individuals and structures) and financial systems of the developed countries. The development of the theory of games in Ukraine is analyzed and it is discovered that there are no specialists who are able to teach students on methods and the technologies, which are used in a market economy. It is noted that the existence of the critical state of information security in the domain of the state of the economy in Ukraine is not even recognized.

УДК 004.415.056.5 (075)

АНАЛІЗ УРАЗЛИВОСТЕЙ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Ігор Павлов

ВІТІ НТУУ "КПІ"

Стаття: ***8 стор., 10 джерел.***

Аналіз існуючих публікацій, пов'язаних з проблемою проектування систем захисту інформації, показує недостатнє освітлення системних підходів до проблеми опису уразливостей систем захисту інформації.

Проводячи різні оцінки ефективності моделей захисту інформації дослідники спираються на окремі підходи до аналізу уразливостей тих або інших систем захисту.

У зв'язку з цим виникає об'єктивна необхідність визначення основних підходів у вивченні процесів, які виникають в областях уразливостей систем захисту інформації під час впливу небезпечних для цих систем загроз. Для цього необхідно визначити місце і роль уразливостей у математичній моделі, провести класифікацію цих уразливостей для подальшого використання системного підходу аналізу уразливостей систем захисту інформації в оцінках ефективності моделей, які будуються на етапі проектування систем захисту інформації. Загальною основою для проведення цього аналізу є модель процесу захисту інформації з повним перекриттям загроз.

У першій частині статті на базі існуючої моделі процесу захисту інформації з повним перекриттям загроз визначаються множини загроз системи захисту та областей захисту. У подальшому множини системи захисту поділяються на окремі множини уразливостей і механізмів захисту. Запропонована математична модель, у якій розкриваються місце і роль уразливостей у системі захисту інформації.

У другій частині статті на базі аналізу різних підходів запропонований системний підхід щодо єдиної класифікації уразливостей систем захисту інформації, який розбивається на складові.

У інформаційних системах існують різні засоби, які використовують різні способи блокування уразливостей систем, попередження впливу загроз на механізми захисту систем захисту інформації. Одним з перспективних напрямків є створення окремих систем виявлення загроз (системи виявлення атак, системи виявлення мережевих втручань і т. п.).

На сьогоднішній день системи виявлення вторгнень являють собою програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються у комп'ютерних системах або мережах, а також самостійно аналізують ці події в пошуках ознак проблем безпеки, в тому числі проводять пошук областей уразливостей систем захисту. Такі системи реалізуються практично в усіх антивірусних системах, які проводять моніторинг програмних інформаційних технологій, встановлених в комп'ютерних системах. Але подальший напрямок розвитку систем, які проводитимуть моніторинг, виявляти та блокувати

уразливості систем захисту інформації та в цілому інформаційних систем, буде розвиватися в напрямку впровадження систем з елементами штучного інтелекту.

АНАЛИЗ УЯЗВИМОСТЕЙ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Игорь Павлов
ВИТИ НТУУ "КПИ"

Анализ существующих публикаций, связанных с проблемою проектирования систем защиты информации, показывает недостаточное освещение системных подходов к проблеме описания уязвимостей систем защиты информации.

Проводя разные оценки эффективности моделей защиты информации исследователи опираются на отрывочные подходы к анализу уязвимостей тех или иных систем защиты.

В связи с этим возникает объективная необходимость определения основных подходов в изучении процессов, возникающих в областях уязвимостей систем защиты информации во время воздействия опасных угроз. Для этого необходимо определить место и роль уязвимостей в математической модели, провести классификацию этих уязвимостей для дальнейшего использования системного похода в анализе уязвимостей систем защиты информации при оценках эффективности моделей, которые разрабатываются на этапе проектирования систем защиты информации. Общей основой для проведения этого анализа является модель процесса защиты информации с полным перекрытием угроз.

В первой части статьи на базе существующей модели процесса защиты информации с полным перекрытием угроз определяются множества угроз, множества входящие в систему защиты и множества областей защиты информационной системы. В дальнейшем множества систем защиты раскрываются на отдельные подмножества уязвимостей и механизмов защиты.

В статье предложена математическая модель, в которой раскрываются место и роль уязвимостей в системах защиты информации.

Во второй части статьи на базе анализа разных подходов предложен системный поход к единой классификации уязвимостей систем защиты информации, которые раскрываются на составляющие.

В информационных системах существуют разные средства, которые используют разные способы блокирования уязвимых мест, предупреждения воздействия угроз на механизмы защиты информации. Одним из перспективных направлений является создание отдельных систем определения угроз (системы выявления атак, системы выявления сетевых вторжений и т. п).

На сегодняшний день системы выявления вторжений представляют собой программные или аппаратно-программные решения, которые автоматизируют процесс контроля действий, протекающий в компьютерных системах или сетях, а также самостоятельно анализируют эти события в поисках признаков проблем безопасности, в том числе проводят поиск областей уязвимости систем защиты. Такие системы реализуются практически во всех антивирусных системах, проводящих мониторинг программных информационных технологий, установленных в компьютерных системах. Дальнейшее направление развития систем, которые проводят мониторинг, выявляют и блокируют уязвимости систем защиты информации и в целом информационных систем, будет заключаться во внедрении систем с искусственным интеллектом.

ANALYSIS OF VULNERABILITIES IN INFORMATION SECURITY SYSTEMS

Igor Pavlov
Military Institute of Telecommunications and Information of the National Technical University of Ukraine "The Kiev polytechnical institute" (MITI NTUU "KPI")

Analysis of existing publications, which are related to the problem of designing information security systems, shows insufficient describing of systematic approaches to description of the vulnerabilities of information security systems.

Researchers rely on tear-off approaches to analyzing technical vulnerabilities or other protection systems during evaluating of the effectiveness of different models of information security.

Accordingly, there is an objective need to identify the main approaches to study the processes that occur in the areas of information security vulnerabilities during influence of hazardous threats to these systems. It is necessary to determine the place and role of vulnerability in a mathematical model to classify these vulnerabilities for further

using of systematic approach to analysis vulnerabilities of information security assessments of performance models that are based on the design phase of protection. The general basis for this analysis is the model of information security threats with complete overlap.

In the first part of the article based on the existing model of information security threats with complete overlap defined set of threats, security system and security areas. In a further set of security system are divided into separate sets of vulnerabilities and protection mechanisms. In the article shows a mathematical model, which reveals the role and place of vulnerabilities in the system of protection.

In the second part of the article, systematic approach is proposed in a single classification of information security vulnerabilities, which divides into components.

Information systems have different tools, which use different methods of locking systems vulnerabilities, prevention threats influence to exposure protection mechanisms of information security systems. Creation of separate systems of threat detection is one of prospective directions (systems detect attacks, detection of network interference, etc.).

Nowadays detection systems represent a software or hardware solutions, which automate the process of monitoring the events, which occurred in a computer system or network, as well as independently analyze these events in the search for signs of security problems, including searching areas of vulnerabilities of protection systems. Such systems are implemented in almost all antivirus systems. But the future direction of development systems, which ' will monitor, detect and block the vulnerability of information security and information systems in general, will develop towards the introduction of elements of artificial intelligence.

УДК 004.057.4:722.4

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ЗАСТОСУВАННЯ МЕРЕЖЕВИХ ПРОТОКОЛІВ ПЕРЕДАЧІ ДАНИХ ДЛЯ ІДЕНТИФІКАЦІЇ, КОНТРОЛЮ ТА АНАЛІЗУ СТАНУ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Ярослав Буригін, Катерина Красовська*, Наталія Тарасова*, Станіслав Боровик*

*Державна служба спеціального зв'язку та захисту інформації України, *Київський національний університет ім. Тараса Шевченка*

Стаття: ***4 стор., 7 джерел***

Сучасний стан розвитку інформаційного суспільства потребує більш тісної інтеграції повсякденного життя людини з інформаційно-комунікаційними технологіями, пов'язаними як з обробкою даних, так і їх передачею. Зважаючи на сильну розгалуженість сучасних інформаційно-телекомунікаційних систем і велику кількість користувачів і обладнання в них, питання щодо забезпечення гарантованої адресації є найголовнішим

Одним зі шляхів забезпечення реалізації процесу передавання, обробки та зберігання інформації в ІТС, а також забезпечення її захисту є використання унікальних ідентифікаторів, таких як: мережева адреса або IP-адреса та фізична адреса або MAC-адреса.

Для відображення фізичної адреси комп'ютера (телекомунікаційного обладнання) в середовище мережевих IP-адрес та навпаки застосовують спеціальні мережеві протоколи, яки дозволяють виконувати цей процес достатньо швидко й зручно. Знаючи IP-адресу та MAC-адресу комп'ютера, можна достатньо чітко ідентифікувати користувача.

Визначення множини мережевих протоколів, які доцільно використовувати для проведення контролю та аналізу стану телекомунікаційного обладнання та збору даних про нього, надасть можливість впливати на ефективність і надійність роботи як телекомунікаційного обладнання, так і ІТС у цілому.

Для перетворення MAC-адрес в адреси мережевого рівня (IP-адреси) і назад застосовуються спеціальні протоколи: ARP, RARP, InARP в мережах IPv4 та NDP в мережах на основі IPv6.

На цей час серед мережевих протоколів, що використовують MAC та IP-адреси, особливої уваги заслуговує протокол ARP: простий, але такий, що має достатній функціонал для об'єднання двох найважливіших унікальних параметрів обладнання в єдину динамічно оновлювану таблицю, що забезпечує більш надійну ідентифікацію телекомунікаційного обладнання.

Крім того, зважаючи, що адміністратор мережі або користувач, застосовуючи певну техніку, програмні засоби і алгоритми, має можливість замість «прошитої» MAC-адреси, призначити телекомунікаційному обладнанню будь-яку іншу MAC-адресу, з метою однозначної ідентифікації користувачів та недопущення їх підміни, пропонуємо дослідити можливість додаткового застосування інших унікальних ідентифікаторів, а саме реєстраційних номерів апаратної частини обладнання або його програмного забезпечення.

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ СЕТЕВЫХ ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ ДЛЯ ИДЕНТИФИКАЦИИ, КОНТРОЛЯ И АНАЛИЗА СОСТОЯНИЯ ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ, В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Ярослав Бурыгин, Катерина Красовская*, Наталия Тарасова*, Станислав Боровик*
*Государственная служба специальной связи и защиты информации Украины *Киевский национальный университет им. Тараса Шевченко*

Современное состояние развития информационного общества нуждается в более тесной интеграции повседневной жизни человека с информационно-коммуникационными технологиями, связанными как с обработкой данных, так и их передачей. Ввиду сильной разветвленности современных информационно-телекоммуникационных систем и большого количества пользователей и оборудования в них, вопрос обеспечения гарантированной адресации является самым главным.

Одним из путей обеспечения реализации процесса передачи, обработки и хранения информации, в информационно-телекоммуникационных системах, а также обеспечение её защиты есть использование уникальных идентификаторов, таких как: сетевой адрес или ip-адрес и физический адрес или MAC-адрес.

Для отображения физического адреса компьютера (телекоммуникационного оборудования) в среду сетевых IP-адресов и наоборот применяют специальные сетевые протоколы, которые позволяют выполнять этот процесс достаточно быстро и удобно. Зная IP-адрес и MAC-адрес компьютера, можно достаточно четко идентифицировать пользователя.

Определение множества сетевых протоколов, которые целесообразно использовать для проведения контроля и анализа состояния телекоммуникационного оборудования и сбора данных о нем, создаст возможность влиять на эффективность и надежность работы, как телекоммуникационного оборудования, так и информационно-телекоммуникационных систем в целом.

Для преобразования MAC-адресов в адреса сетевого уровня (IP-адреса) и назад применяются специальные протоколы: ARP, RARP, INARP в сетях Ipv4 и NDP в сетях на основе Ipv6.

В настоящее время среди сетевых протоколов, которые используют MAC и IP-адреса, особого внимания заслуживает протокол ARP: простой, но такой, который имеет достаточный функционал для объединения двух важнейших уникальных параметров оборудования в единственную динамически обновляемую таблицу, которая обеспечивает более надежную идентификацию телекоммуникационного оборудования.

Кроме того, принимая во внимание, что администратор сети или пользователь, применяя определенную технику, программные средства и алгоритмы, имеет возможность вместо «прошитого» MAC-адреса, назначить телекоммуникационному оборудованию любой другой MAC-адрес, с целью однозначной идентификации пользователей и недопущения их подмены, предлагаем исследовать возможность дополнительного применения других уникальных идентификаторов, а именно регистрационных номеров аппаратной части оборудования или его программного обеспечения.

RESEARCHSNG POSSIBILITIES OF APPLICATION OF NETWORK TRANSMISSION PROTOCOL FOR IDENTIFYING, MONITORING AND ANALYSIS OF TELECOMMUNICATIONS EQUIPMENT IN INFORMATION AND TELECOMMUNICATION SYSTEMS

Jaroslav Buryhin, Catherine Krasovska*, Natalia Tarasova*, Stanislav Borovik*
*State Service for Special Communication and Information Protection of Ukraine, *Taras Shevchenko Kyiv National University*

The current state of development of the information society requires closer integration of everyday life with information and communication technology, which is related to data processing and transmission. Given the fact of strong branching of advanced ITS and a large number of users and the equipment in them, the sharpest issue is providing guaranteed addressing.

One of the ways to ensure the realization of the process of transmission, processing and storage of information in the ITS, and the provision of information security, is the use of unique identifiers such as network address or IP-address and the physical address or MAC- address .

To display the physical address of the computer (telecommunications equipment) in the environment of network IP- addresses and vice versa are used special network protocols, which allow to perform this process quite quickly and conveniently. Knowing the IP- address and MAC- address of the computer you can identify the user quite clearly.

Defining the set of network protocols that should be used for monitoring and analysis of telecommunications equipment and data collection of it will allow to influence on the efficiency and reliability of both telecommunications equipment and ITS in general.

To convert a MAC- addresses to network layer addresses (IP addresses) is using special protocols: ARP, RARP, InARP IPv4 networks and NDP networks based on IPv6.

At present, among the network protocols that use the MAC and IP addresses, special attention should pay to Protocol ARP: it is simple, but one that has enough functionality to combine two the most important unique parameters of equipment in a single dynamically updated table that provides a reliable identification of telecommunications equipment.

Furthermore, given that the network administrator or the user, using a technique, software tools and algorithms, is able instead of "Stitched" MAC- addresses to assign for telecommunications equipment any other MAC- address, in order to uniquely identify users and prevent any substitution, we offer to explore the possibility of additional use of other unique identifiers, such as the registration number of hardware or software.

УДК 681.3.067

ЗАХИЩЕНА ВЕБ-СИСТЕМА ТЕСТУВАННЯ ЯКОСТІ ЗНАНЬ З ВИКОРИСТАННЯМ АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ ТЕХНОЛОГІЙ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Юрій Яремчук
Вінницькій національний технічний університет

Стаття: ***8 стор, 17 джерел.***

Наразі тестування є найбільш сучасним методом контролю знань. Суттєвим недоліком сучасних комп'ютерних систем тестування є їхня прив'язка до платформи та операційної системи, на яких вона реалізована. Окрім цього існує проблема безпеки систем тестування, оскільки кожна операційна система має свої власні вразливості, які можуть впливати на роботу програмного продукту. Тому актуальною стала розробка такої системи тестування, яка б забезпечувала надійний захист тестування і при цьому мала гнучку систему доступу кандидатів до системи тестування, без прив'язування до конкретної платформи чи операційної системи. Запропоновано реалізацію системи тестування з використанням крос-платформних рішень, які мають широкі можливості щодо побудови захищених систем з високим рівнем безпеки, а також

веб-технологій, що дозволяє використовувати систему тестування на будь-якому пристрої, що підключений до глобальної мережі Інтернет або локальної мережі з використанням власного веб-серверу. Представлено структурну схему захищеної веб-системи тестування, а також взаємозв'язки між її компонентами. Розглянуто особливості розробки кожного програмного модуля веб-системи тестування. Розглянуто проблеми забезпечення безпеки системи тестування, а також можливі атаки зловмисника. Розроблено механізми захисту бази даних та даних, що передаються в системі тестування. Усі необхідні технології криптографічного захисту, як то шифрування, ключового обміну, автентифікації та цифрового підписування, розроблено на основі власних методів на єдиному математичному апараті рекурентних V_k –послідовностей. Це дозволило не лише підвищити рівень безпеки системи тестування, але й підвищити швидкість виконання в ній криптографічних перетворень.

ЗАЩИЩЕННАЯ ВЕБ-СИСТЕМА ТЕСТИРОВАНИЯ КАЧЕСТВА ЗНАНИЙ С ИСПОЛЬЗОВАНИЕМ АССИМЕТРИЧЕСКИХ КРИПТОГРАФИЧЕСКИХ ТЕХНОЛОГИЙ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Юрий Яремчук
Винницкий национальный технический университет

На сегодня тестирование является наиболее современным методом контроля знаний. Существенным недостатком современных компьютерных систем тестирования является их привязка к платформам и операционным системам, на которых она реализована. Кроме этого существует проблема безопасности систем тестирования, поскольку каждая операционная система имеет свои собственные уязвимости, которые могут влиять на роботу программного продукта. Поэтому актуальной становится разработка такой системы тестирования, которая бы обеспечивала надежную защиту тестирования и при этом имела гибкую систему доступа кандидатов к системе тестирования, без привязки к конкретной платформе или операционной системе. Предложено реализацию системы тестирования с использованием кросс-платформенных решений, которые имеют широкие возможности для построения защищенных систем с высоким уровнем безопасности, а также веб-технологий, позволяющих использовать систему тестирования на любом устройстве, подключенном к глобальной сети Интернет или локальной сети с использованием собственного веб-сервера. Представлено структурную схему защищенной веб-системы тестирования, а также взаимосвязи между ее компонентами. Рассмотрены особенности разработки каждого программного модуля веб-системы тестирования. Рассмотрены проблемы обеспечения безопасности системы тестирования, а также возможные атаки злоумышленника. Разработаны механизмы защиты базы данных и данных, которые передаются в системе тестирования. Все необходимые технологии криптографической защиты, как то шифрования, ключевого обмена, аутентификации и цифрового подписания разработаны на основе собственных методов на едином математическом аппарате рекуррентных V_k –последовательностей. Это позволило не только повысить уровень безопасности системы тестирования, но и повысить скорость выполнения в ней криптографических преобразований.

SECURE WEB-SYSTEM OF KNOWLEDGE QUALITY TESTING WITH ASYMMETRIC CRYPTOGRAPHIC TECHNOLOGIES BASED ON RECURRENT SEQUENCES

Yuriy Yaremchuk
Vinnytsia national technical university

At present, testing is the most modern method of knowledge control. A significant drawback of modern computer testing systems is their attachment to the platform and operating system on which it is implemented. In addition, there is a problem of testing system security, since each operating system has its own vulnerabilities that may affect the operation of the software. Therefore, it became urgent to develop such a testing system, which provides reliable protection for testing and has a flexible access system of candidates to the testing system without linking to a particular platform or operating system. We suggested implementation of the testing system using a cross-platform solutions that have ample opportunities to build secure systems with high security level, and web-

technologies allowing the use of the testing system for any device connected to the Internet or LAN using one's own web-server. We presented a structural scheme of the secure web-based testing system and relationship between its components. We considered development features of each software module of the web-based testing system. We considered problems of security provision for the testing system, and possible malicious attacks. We developed protection mechanisms for databases and the data transmitted in the testing system. All required cryptographic protection technologies, such as encryption, key exchange, authentication and digital signature were developed on the basis of own methods on a single mathematical apparatus of recurrent V_k sequences. This allowed us not only to improve the testing system security, but also to increase its speed of cryptographic transformations.

УДК 004.056:004.451.1(045)

ЗАХИСТ І МОНІТОРИНГ ПОРТІВ УВЕДЕННЯ ВИВЕДЕННЯ В ОПЕРАЦІЙНИХ СИСТЕМАХ LINUX

Сергій Єгоров
Національний авіаційний університет

Стаття: ***7 стор., 4 джерела.***

Служби – це фундаментальна складова мережного робочого середовища комп'ютерів. Якби не було служб, то в комп'ютері можна було б запускати не більше однієї програми, до якої можна було б підключатися клієнтам по одному за раз. В основі роботи служб лежить концепція портів. Порт – це спеціальна добавка до IP-адреси, яка дозволяє визначити серверу, як саме працювати із клієнтською частиною. Більшість користувачів дуже погано знайома з портами, не говорячи вже про механізм їх функціонування. Це пов'язано з тим, що для роботи з мережею необхідно знати тільки IP-адресу, а номер порту знати не обов'язково, бо цей номер запрограмований усередині програми. Однак знання загальних правил роботи служб і портів веде до розуміння основних концепцій безпеки. Метою даної статті є розробка рекомендацій щодо аналізу стану портів операційної системи Linux і забезпечення їх захисту. Як приклад використалася операційна система Linux Ubuntu 13.10 (64 bit), яка працювала як гостьова операційна система під керуванням Windows 7 (64 bit).

Відстеження стану портів операційної системи дозволяє коректно настроїти фаервол, а також у деяких випадках і запобігти хакерській атаці або виявити канал витоку інформації й вжити адекватних заходів. Для адекватного настроювання й супроводу операційної системи також слід знати й методи злому операційних систем. Єдиний спосіб адекватно настроїти й супроводжувати фаерфол – використовувати методику відстеження стану портів.

ЗАЩИТА И МОНИТОРИНГ ПОРТОВ ВВОДА ВЫВОДА В ОПЕРАЦИОННЫХ СИСТЕМАХ LINUX

Сергей Егоров
Национальный авиационный университет

Службы – это фундаментальная составляющая сетевой рабочей среды компьютеров. Если бы не было служб, то в компьютере можно было бы запускать не белее одной программы, к которой можно было бы подключаться клиентам по одному за раз. В основе работы служб лежит концепция портов. Порт – это специальная добавка к IP-адресу, которая позволяет определить серверу, как именно работать с клиентской частью. Большинство пользователей очень плохо знакомы с портами, не говоря уже о механизме их функционирования. Это связано с тем, что для работы с сетью необходимо знать только IP-адрес, а номер порта знать не обязательно, потому что этот номер запрограммирован внутри программы. Однако знание общих правил работы служб и портов ведёт к пониманию основных концепций безопасности. Целью данной статьи является разработка рекомендаций относительно анализа состояния портов операционной системы Linux и обеспечения их защиты. В качестве примера использовалась операционная система Linux Ubuntu 13.10 (64 bit), которая работала как гостевая операционная система под управлением Windows 7 (64 bit).

Отслеживание состояния портов операционной системы позволяет корректно настроить фаервол, а также в некоторых случаях и предотвратить хакерскую атаку или выявить канал утечки информации и принять

адекватные меры. Для адекватной настройки и сопровождения операционной системы также следует знать и методы взлома операционных систем. Единственный способ адекватно настроить и сопровождать фаерфол – использовать методику отслеживания состояния портов.

THE PROTECTION AND MONITORING OF INPUT OUTPUT PORTS IN LINUX OPERATING SYSTEMS

Serhii Yehorov
National Aviation University

Services - is a fundamental component of network computer environment. If there were no services, the computer could not run the whiter one program, which could be connected to customers one at a time. The basis of the services is the concept of ports. Port - a special supplement to the IP-address, which allows the server to determine exactly how to work with the client part. Most people are very uncomfortable with the ports, not to mention the mechanism of their functioning ports. This is due to the fact that for the network only need to know IP-address and the port number does not necessarily know because this number has been programmed within the program. However, knowledge of the general rules of the services and ports leads to an understanding of the basic concepts of security. The purpose of this paper is to develop recommendations for the analysis of the ports the Linux operating system and ensure their protection. As an example, the operating system used by Linux Ubuntu 13.10 (64 bit), who worked as a guest operating system running Windows 7 (64 bit).

Tracking the status of ports operating system can correctly configure the firewall, as well as in some cases, prevent hacker attack or identify channel information leakage and take adequate measures. To configure and maintain adequate operating system should also be aware and hacking techniques operating systems. The only way to properly configure and maintain faerfol - use a technique tracking the serial ports.

УДК 621.396.4

ФОРМИРОВАНИЕ И ОБРАБОТКА ШУМОПОДОБНЫХ СИГНАЛОВ В СТАНЦИИ ТРОПОСФЕРНОЙ СВЯЗИ

Дмитрий Вергелес, Геннадий Леоненко, Андрей Паламарчук, Алексей Юдин
ГосНИИ Спецсвязи

Стаття: ***5 стор., 9 джерел.***

Один из методов борьбы с межсимвольной интерференцией и повышения энергетической эффективности заключается в использовании шумоподобных сигналов (ШПС). Произведение длительности этих сигналов на занимаемую полосу (база ШПС), значительно больше единицы и может лежать в пределах 10 до 10^4. ШПС имеют свойства «сжатия» в базу раз, что и определяет их использование для повышения энергетической эффективности и устранения влияния межсимвольной интерференции на устойчивость тропосферной связи.

В то же время ШПС имеют много специфических особенностей и свойств, без учета которых невозможно правильно их использовать для повышения энергетической эффективности станции тропосферной связи.

При выборе ШПС, кроме временных и частотных характеристик, необходимо знать их автокорреляционные и взаимно корреляционные характеристики. Как правило ШПС построены с использованием линейных рекуррентных последовательностей (ЛРП). Наибольшее распространение получили последовательности Хаффмена, поскольку имеют хорошие корреляционные свойства и просты в формировании. Для переноса ШПС на радиочастоту могут использоваться различные виды модуляции. Для линий тропосферной связи используется фазовая манипуляция (ФМн).

Фаза ФМн сигналов, сформированных на основе последовательностей Хаффмена, принимает значения 0 или π. Определения базы ШПС производится после предварительного расчета радиолинии тропосферной связи исходя из необходимого значения отношения энергии сигнала к спектральной плотности мощности шума h^2.

Учитывая статистические характеристики коэффициентов передачи канала тропосферной связи в частотной и временной областях для обработки ШПС в станциях тропосферной связи необходимо использовать согласованные фильтры (СФ), работающие на радиочастоте.

Это обусловлено тем, что СФ инвариантен относительно задержки сигнала и его начальной фазы (насколько эта величина изменяется в сигнале на входе фильтра, настолько она изменяется и в сигнале на выходе), а коррелятор не инвариантен. При использовании согласованного фильтра имеет место сжатие сигнала во временной области и амплитуда сигнала на выходе согласованного фильтра возрастает в базу раз.

Процедура синтеза СФ сводится к созданию дискретной задерживающей системы, фазированию задержанных во времени сигналов и их суммированию.

Наиболее эффективно реализовать СФ на поверхностных акустических волнах (ПАВ). При таком способе реализации достигаются предельные параметры СФ, определяемые исходя из значения h^2, как известно, связанного с базой сигнала соотношением $h^2=P_c/P_n*Б_c$.

ФОРМУВАННЯ ТА ОБРОБКА ШУМОПОДІБНИХ СИГНАЛІВ У СТАНЦІЇ ТРОПОСФЕРНОГО ЗВ'ЯЗКУ

Дмитро Вергелес, Геннадій Леоненко, Андрій Паламарчук, Олексій Юдін
ДержНДІ Спецзв'язку

Один із методів боротьби з міжсимвольною інтерференцією та підвищенням енергетичної ефективності полягає в використанні шумоподібних сигналів (ШПС). Добуток тривалості цих сигналів на зайняту смугу (база ШПС) значно більше одиниці та може знаходитись в межах від 10 до 10^4. ШПС мають властивості «стискання» в базу разів, що і обумовлює їх використання для підвищення енергетичної ефективності та усунення впливу міжсимвольної інтерференції на стійкість тропосферного зв'язку.

В той же час, ШПС мають багато специфічних особливостей та властивостей, без урахування яких неможливо правильно їх використовувати для підвищення енергетичної ефективності при розробці апаратури станції тропосферного зв'язку.

Під час вибору ШПС, окрім часових та частотних характеристик, необхідно знати їх автокореляційні та взаємно кореляційні характеристики. Як правило, ШПС побудовані з використанням лінійних рекурентних послідовностей (ЛРП). Найбільше поширення отримали послідовності Хаффмена, оскільки вони мають хороші кореляційні властивості та прості в формуванні. Для переносу ШПС на радіочастоту можуть використовуватися різні види модуляції. Для ліній тропосферного зв'язку використовується фазова маніпуляція (ФМн).

Фаза ФМн сигналів, сформованих на базі послідовностей Хаффмена, приймає значення 0 або π. Визначення бази ШПС здійснюється після попереднього розрахунку радіолінії тропосферного зв'язку виходячи з необхідного значення співвідношення енергії сигналу до спектральної щільності потужності шуму h^2.

Враховуючи статистичні характеристики коефіцієнтів передачі каналу тропосферного зв'язку в частотній та часовій областях для обробки ШПС в станціях тропосферного зв'язку необхідно використовувати узгоджені фільтри (УФ), які працюють на радіочастоті.

Це обумовлено тим, що УФ інваріантний відносно затримки сигналу і його початкової фази (наскільки ця величина змінюється в сигналі на вході фільтру, настільки вона змінюється і в сигналі на виході), а корелятор не інваріантний. При використанні узгодженого фільтру має місце стискання сигналу в часовій області і амплітуда сигналу на виході узгодженого фільтру збільшується у базу разів.

Процедура синтезу УФ зводиться до створення дискретної системи з затримкою, фазування затриманих в часі сигналів та їх підсумовування.

Найбільш ефективно реалізовувати УФ на поверхневих акустичних хвилях (ПАХ). При такому способі реалізації досягаються граничні параметри УФ, які визначаються виходячи з значення h^2, як відомо, пов'язаного з базою сигналу співвідношенням $h^2=P_c/P_n*Б_c$.

FORMATION AND PROCESSING OF NOISE-LIKE SIGNALS IN THE TROPOSPHERIC COMMUNICATION

Dmitro Vergeles, Gennady Leonenko, Andriy Palamarchuk, Oleksii Yudin
SRI for STIP

One of methods of a struggle with an intersymbol interference and raises of energetic efficiency, consists in usage noise-like signals (NLS). Production of duration of these signals on an occupied band (basis NLS), much more unit also can lie within 10 to 10^4. NLS have properties of "compression" in basis of times, as defines their usages for raise

of energetic efficiency and elimination of agency of an intersymbol interference on a stability of tropospheric connection.

In too time NLS have many specific singularities and properties without which registration it is impossible to use correctly them for raise of energetic efficiency by development of equipment of tropo relay station.

At choice NLS, except temporal and frequency responses, it is necessary to know their autocorrelated and mutually correlative performances. As a rule NLS are built with usage of the linear recurrent sequences (LRS). The greatest propagation was gained by sequences of Haffmen as have good correlative properties and are simple in shaping. For transfer NLS on a radio-frequency various types of modulation can be used. For lines of tropospheric communication phase manipulation is used (PM).

At PM the signals generated on the basis of sequences of Haffmen, a phase accepts values 0 or π. Determinations of basis NLS it is made after predesign of a radio frequency spectral line of tropospheric connection proceeding from necessary value of the ratio of energy of a signal to spectral density of noise power h^2.

Considering statistical performances of transfer efficiencies of the channel of tropospheric connection in the frequency and temporal areas for handling NLS in tropo relay stations it is necessary to use the matched filters (MF) working on a radio-frequency.

It is caused by that the MF is invariant concerning signal delay and its starting phase (how much this value varies in a signal on a filter input, so it varies and in a signal on an output), and the correlator is not invariant. At usage of the matched filter signal compression in temporal area occurs and signal amplitude on an output of the matched filter increases in basis of times.

Procedure of synthesis of MFis reduced to creation of discrete delaying system, phasing of the signals delayed in a time and to their summation.

Most effectively to implement MF on acoustic surface waves (ASW). At such method of implementation limiting parameters of MF, defined proceeding from value h^2 and, as it is known, h^2 it is connected with base of a signal a parity h^2=Рс/Рп*Бс.

УДК 621.372

ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ВІД ВИТОКУ ЗА РАХУНОК ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ТА НАВЕДЕНЬ ПРИ ПОШИРЕННІ В ДОСЛІДЖУВАНИХ КОЛАХ ТЕСТОВИХ СИГНАЛІВ

Михайло Прокофьєв, Василь Стеченко
НДЦ «ТЕЗІС» НТУУ КПІ

Стаття ***6 стор., 6 джерел***

Засобами обчислювальної техніки інформація обробляється у вигляді електричних імпульсних сигналів. Цей процес супроводжується випромінюванням в навколишній простір змінного електромагнітного поля, яке дистанційно може перехоплюватися і розшифровуватися засобами технічної розвідки.

Критерієм оцінювання якості передавання інформації, в тому числі і неможливості її відновлення, є ймовірність її правильного прийому. Імовірність в свою чергу визначається відношенням енергії імпульсного сигналу в точці його прийому до спектральної щільності шуму.

Рівень побічного випромінювання зазвичай наближається до рівня навколишнього шуму, тому оцінюванню підлягають параметри каналу зв'язку з низьким співвідношенням сигнал/шум. Вимірювання енергії одиночного сигналу малого рівня – це складне і практично не реалізоване завдання. Тому оцінювання захищеності інформації проводять при передаванні в досліджуваних колах тестових періодичних сигналів. Заміна одиночного імпульсу з безперервним спектром на періодичну послідовність імпульсів дозволяє за рахунок високої селективності вимірювального приладу виявити і виміряти малі рівні гармонік тестового сигналу на тлі шуму що заважає.

У той же час для оцінювання рівня захищеності переданої інформації необхідно порівнювати енергію одиночного імпульсного сигналу з рівнем шуму. Показано, що енергія імпульсного сигналу що випромінюється практично рівномірно розподілена в смузі частот, шириною більше трьох октав. Тому оцінювання відносини сигнал/шум на дискретних гармоніках періодичного тестового сигналу не враховує зміну спектра імпульсу в процесі його випромінювання, нерівномірний рівень шуму в смузі прийому і може істотно відрізнятися від такої ж оцінки для одиночного імпульсу.

У статті показаний перехід від інтегрального відношення сигнал/шум, яке справедливе для оцінювання ймовірності правильного приймання одиночного імпульсного сигналу, до наближеною оцінки на дискретних гармоніках періодичного тестового сигналу. Показано можливість підвищення точності такої оцінки шляхом збільшення щільності імпульсів тестового сигналу.

ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ УТЕЧКИ ЗА СЧЕТ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК ПРИ РАСПРОСТРАНЕНИИ В ИССЛЕДУЕМЫХ ЦЕПЯХ ТЕСТОВЫХ СИГНАЛОВ

Михайло Прокофьєв, Василий Стеченко
НДЦ «ТЕЗИС» НТУУ КПИ

Средствами вычислительной техники информация обрабатывается в виде электрических импульсных сигналов. Этот процесс сопровождается излучением в окружающее пространство переменного электромагнитного поля, которое дистанционно может перехватываться и расшифровываться средствами технической разведки.

Критерием оценки качества передачи информации, в том числе и невозможности ее восстановления, является вероятность ее правильного приема. Вероятность в свою очередь определяется отношением энергии импульсного сигнала в точке его приема к спектральной плотности мешающего шума.

Уровень побочного излучения обычно соизмерим с уровнем окружающего шума, поэтому оценке подлежат параметры канала связи с низким соотношением сигнал/шум. Измерение энергии одиночного сигнала малого уровня – это сложная и практически нереализуемая задача. Поэтому оценку защищенности информации проводят при передаче в исследуемых цепях тестовых периодических сигналов. Замена одиночного импульса с непрерывным спектром на периодическую последовательность импульсов позволяет за счет высокой селективности измерительного прибора выявить и измерить малые уровни гармоник тестового сигнала на фоне мешающего шума.

В тоже время для оценки уровня защищенности передаваемой информации необходимо сравнивать энергию одиночного импульсного сигнала с уровнем мешающего шума. Показано, что энергия излученного импульсного сигнала практически равномерно распределена в полосе частот, шириною более трех октав. Поэтому оценка отношения сигнал/шум на дискретных гармониках периодического тестового сигнала не учитывает изменение спектра импульса в процессе его излучения, неравномерный уровень мешающих помех в полосе приема и может существенно отличаться от такой же оценки для одиночного импульса.

В статье показан переход от интегрального отношения сигнал/шум, справедливого для оценки вероятности правильного приема одиночного импульсного сигнала, к приближенной оценке на дискретных гармониках периодического тестового сигнала. Показана возможность повышения точности такой оценки путем увеличения скважности импульсов тестового сигнала.

ESTIMATION OF SECURITY AGAINST LEAKAGE DUE TO COMPROMISING EMANATIONS PROPAGATING IN INVESTIGATED CIRCUITS TEST SIGNAL

Mikhail Prokofiev, Vasil Stechenko
SRC "TESIS" NTUU "KPI"

Computer equipment information is processed in the form of electrical pulse signals . This process is accompanied by the emission into the environment variable electromagnetic field , which can be remotely intercepted and decrypted by means of technical intelligence .

The criterion for evaluating the transmission quality information , including an inability to restore a probability of correct reception . Chance in turn determined by the ratio of the pulse signal energy at the point of admission to the spectral density of the interfering noise.

Spurious usually commensurate with the level of ambient noise , so shall be evaluated parameters of the channel due to low signal / noise ratio . Measuring the energy of a single low-level signal - it is a complicated and practically impossible task. Therefore, assessment of data protection is carried out at the transfer test in the test circuits periodic

signals. Replacement of a single pulse with a continuous spectrum on a periodic sequence of pulses allows high selectivity due to the measuring device to detect and measure low levels of harmonics of the test signal to background noise disturbance .

At the same time to assess the level of information security is necessary to compare the energy of a single pulse with the level of the interfering noise. It is shown that the energy of the emitted pulse almost uniformly distributed in the frequency band width of more than three octaves . Therefore, the evaluation of the signal / noise ratio at discrete harmonics periodic test signal does not account for the change of the pulse spectrum in the process of radiation , preventing uneven level of interference in the reception and may differ significantly from the same estimates for a single pulse .

The article shows the transition from the integral ratio of the signal / noise ratio, which is valid for estimating the probability of correct reception of a single pulse signal to an approximate evaluation of discrete harmonics periodic test signal . The possibility of increasing the accuracy of such estimates by increasing the duty cycle of the test signal .

УДК 621.396.4

МЕТОДИ СТРУКТУРНОЇ НАДІЙНІСТІ МУЛЬТИСЕРВІСНИХ МЕРЕЖ ЗВ'ЯЗКУ

Дмитро Могилевич, Валерій Правило, Микола Фомін
ВІТІ ДУТ

Стаття: ***5 стор, 11 джерел***

Розвиток інформаційних послуг, який спостерігається протягом усього періоду існування телекомунікаційної індустрії, відбувається за двома основними напрямами: поява принципово нових послуг і підвищення вимог до якості вже існуючих послуг. Сучасні телекомунікаційні мережі являють собою різновид об'єктів технічного проектування і можуть створюватися «з нуля» або розвиватися на основі існуючих рішень. Незалежно від цього етапам технічної реалізації передує, як правило, етап моделювання з метою визначення тих чи інших параметрів мережі, важливе місце серед яких займає структурна надійність мережі. У таких випадках виникає необхідність у розгляді методів оцінки структурної надійності мережі загалом, а також окремих її зв'язків. Такі методи корисні і в разі оцінки надійності структурно складних мереж із заданою структурою, коли застосування відомих методів утруднене або неможливе. Тому розгляд можливісті застосування наближених методів структурної надійності для оцінки мультисервісних мереж спеціального призначення є актуальним.

Як один зі способів оцінки структурної надійності мережі запропоновано оцінювати її на підставі методу двосторонньої оцінки структурної надійності на основі оцінок Езарі-Прошана. Використання цього методу дає змогу здебільшого істотно скоротити обсяг обчислень, необхідних для одержання оцінки із заданою точністю. Практичне застосування того або іншого методу визначається постановкою завдання, наявним парком обчислювальної техніки, ступенем точності вихідних ймовірностей безвідмовного обслуговування заявок на елементах і розмірністю оцінюваної телекомунікаційної системи.

МЕТОДЫ СТРУКТУРНОЙ НАДЕЖНОСТИ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ

Дмитрий Могилевич, Валерий Правило, Николай Фомин
ВИТИ ГУТ

Развитие информационных услуг, которое наблюдается в течение всего периода существования телекоммуникационной индустрии, происходит по двум основным направлениям: появление принципиально новых услуг и повышение требований к качеству существующих услуг. Современные телекоммуникационные сети представляют собой разновидность объектов технического проектирования и могут создаваться «с нуля» или развиваться на основе существующих решений. Независимо от того этапам технической реализации предшествует, как правило, этап моделирования с целью определения тех или иных параметров сети, важное место среди которых занимает структурная надежность сети. В таких случаях возникает необходимость в рассмотрении методов оценки структурной надежности сети в целом, а также отдельных ее связей. Такие методы полезны и при оценке надежности структурно сложных сетей с заданной структурой, когда применение известных методов затруднено или невозможно. Поэтому рассмотрение

возможности применения приближенных методов структурной надежности для оценки мультисервисных сетей специального назначения является актуальным. Как один из способов оценки структурной надежности сети предложено оценивать ее на основании метода двусторонней оценки структурной надежности на основе оценок Эзари - Прошана. Использование этого метода позволяет, в основном, существенно сократить объем вычислений, необходимых для получения оценки с заданной точностью. Практическое применение того или иного метода определяется постановкой задачи, имеющимся парком вычислительной техники, степенью точности исходных вероятностей безотказного обслуживания заявок на элементах и размерностью оцениваемой телекоммуникационной системы.

METHODS OF STRUCTURAL RELIABILITY MULTISERVICE COMMUNICATION NETWORKS

Dmitro Mogilevich, Valeriy Pravilo, Mykola Fomin
MITI SUT

The development of information services, which is observed throughout the duration of the telecommunications industry, is in two main areas: the emergence of innovative services and increase the quality requirements of existing services. Modern telecommunications networks are a kind of engineering design objects and can be created "from scratch" and develop on the basis of existing solutions. Regardless of the technical implementation of this phase is preceded usually stage modeling to identify certain network parameters, important among which covers the structural reliability of the network. In such cases, there is a need for consideration of methods for assessing the structural reliability of the network as a whole and its individual links. Such methods are useful in the case of structural reliability assessment of complex networks with a given structure, where the application of known methods is difficult or impossible. Therefore, consideration of the possibility of using approximate methods of structural reliability assessment for multi-service networks , special purpose is relevant.As one way to assess the structural reliability of the network is proposed to assess it on the basis of bilateral assessment method based on structural reliability assessments Ezari - Proshana. Using this method allows for the most part significantly reduce the amount of computation required to obtain estimates with a given accuracy. Practical application of a particular method is defined statement of the problem, the existing fleet of computer technology, the degree of accuracy the probability of failure of initial requests for service elements and the dimension of the estimated telecommunication system.

УДК 004.056.53(045)

НОВІТНІ МЕТОДИ АУТЕНТИФІКАЦІЇ В БЕЗДРОТОВИХ СИСТЕМАХ ТА МЕРЕЖАХ

Анна Чунарьова , Руслана Зюбіна
Національний авіаційний університет

Стаття: ***6 стор., 8 джерел.***

Наразі бездротові технології розвиваються в напрямку на спрощення доступу до інформаційних ресурсів глобальної мережі та дають можливість побудови універсальних локальних мереж на основі стандартів IEEE 802.11 та IEEE 802.16. Одним із рубежів безпеки в бездротових мережах є ідентифікація та автентифікація користувачів. Відповідно до стандарту IEEE 802.11 існує три базових режими безпеки, що вибираються бездротовим пристроєм в залежності від рівня секретності: відкритий режим; захищений режим без автентифікації, але з шифруванням трафіку; захищений режим з автентифікацією і шифруванням трафіку. Впровадження правил розмежування доступу до інформаційних ресурсів бездротових мережі пояснюється масовістю використання бездротових технологій. Використання та розширення радіодіапазону збільшує ймовірність порушення атрибутів конфіденційності, цілісності та доступності оброблюваної інформації. Тому використання автентифікації для захисту інформаційних ресурсів є досить актуальною задачею з точки зору забезпечення базових властивостей та розмежування прав доступу.

Основними стандартами автентифікації в бездротових мережах є стандарти IEEE 802.11, WPA, WPA2 та IEEE 802.1x. Базовими уразливостями безпеки бездротових мереж є: проблеми ідентифікатора SSID бездротової локальної мережі; уразливість відкритої автентифікації; уразливість автентифікації із спільним ключем; уразливість автентифікації за MAC- адресою.

У даній статті проведено аналіз стандартів автентифікації в сучасних бездротових мережах. На основі проведеного аналізу в статті розроблено рекомендацій щодо використання новітніх методів аутентифікації користувачів в сучасних бездротових мереж та запропонована множина захисних функцій автентифікації на базі еліптичних кривих.

НОВЕЙШИЕ МЕТОДЫ АУТЕНТИФИКАЦИИ В БЕСПРОВОДНЫХ СИСТЕМАХ И СЕТЯХ

Анна Чунарева, Руслана Зюбина
Национальный авиационный університет

Сегодня беспроводные технологии направлены на упрощение доступа к информационным ресурсам глобальной сети и дают возможность построения универсальных локальных сетей на основе стандартов IEEE 802.11 и IEEE 802.16. Одним из рубежей безопасности в беспроводных сетях является идентификация и аутентификация пользователей. Согласно стандарту IEEE 802.11 существует три базовых режима безопасности, выбираются беспроводным устройством в зависимости от уровня секретности: открытый режим; защищенный режим без аутентификации, но шифрованием трафика; защищенный режим с аутентификацией и шифрованием трафика. Внедрение правил разграничения доступа к информационным ресурсам беспроводных сети объясняется массовостью использования беспроводных технологий. Использование и расширение радиодиапазона увеличивает вероятность нарушения атрибутов конфиденциальности, целостности и доступности обрабатываемой информации. Поэтому использование аутентификации для защиты информационных ресурсов является весьма актуальной задачей с точки зрения обеспечения базовых свойств и разграничения прав доступа.

Основными стандартами аутентификации в беспроводных сетях являются стандарты IEEE 802.11, WPA, WPA2 и IEEE 802.1x. Базовыми уязвимостями безопасности беспроводных сетей являются: проблемы идентификатора SSID беспроводной локальной сети; уязвимость открытой аутентификации; уязвимость аутентификации с общим ключом; уязвимость аутентификации по MAC-адресу.

В данной статье проведен анализ стандартов аутентификации в современных беспроводных сетях. На основе проведеного анализа разработаны рекомендации по использованию новейших методов аутентификации пользователей в современных беспроводных сетей и предложено множество защитных функций аутентификации на базе эллиптических кривых.

NEW METHODS OF AUTHENTICATION IN THE WIRELESS SYSTEMS AND NETWORKS

Anna Chunareva, Ruslana Zyubina
National Aviation University

Electronic digital signature (EDS) is a complete analogue of the usual electronic signatures on paper, but it is not implemented with the help of graphics, but with the help of mathematical transformations on the contents of the document. Features a mathematical algorithm to create and verify digital signature ensures the impossibility of such a signature forgery by third parties, provides property nevidmovnosti of authorship. Reliability and ease of use of a digital signature is unmistakable. The procedure for checking the signature executed by a computer error-free, thus avoiding the human factor in the normal signature verification. EDS provides information not only about the person signing the document (the authenticity of the message), but also to verify that the document has not been altered or tampered with after signing (integrity of the document). Also one of the optional components of EDS is a time stamp that shows the actual time of signing the document as opposed to the date specified in the document itself.

This article analyzes the authentication standards in modern wireless networks. Based on the analysis to develop recommendations for the use of innovative user authentication methods in modern wireless networks and proposed a variety of protective functions of authentication on elliptic curves.