ка наблюдается в процедуре установления соединения IMS-IMS, в ходе которого на элемент S-CSCF поступает поток заявок, интенсивность которого в 45 больше, чем начальная.

Подход построения аналитической модели с использованием теоремы BCMP сети хорошо себя зарекомендовал, он значительно упрощает расчет и улучшает наглядность результатов расчета.

Литература

1. Гольдштейн Б.С. Справочник по телекоммуникационным протоколам: протокол SIP / Б.С. Гольдштейн, А.А. Зарубин, В.В. Саморезов.- СПб.: БХВ-Петербург, 2007.

2. Гамиль А.А., Куликов Н.А. Построение модели задержки сигнального трафика в сети связи на базе подсистемы IMS // Электросвязь – 2014. – № 9.

3. Кутбитдинов С. Ш. Концептуальная модель процесса установления соединения в подсистеме IMS / С. Ш.Кутбитдинов // Инфокоммуникации: Сети-Технологии-Решения.-2011,-№ 1.-С. 5-13.

Нурматова Севара Батыровна
Старший преподаватель кафедры «Сети и системы передачи данных» (С и СПД) Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий (ТУИТ)
Тел.: +998 (94) 603-20-77, +998 (71) 238-65-83
Эл. почта: sevara-mmm@inbox.ru

Nurmatova S.B.

Analytical Design of Procedure of re-Registering in IMS

It is onsidered functional diagram of establishment of connection in IMS of technology, feature of re-registering of subscribers; it is also shown an analytical design over of an alarm traffic for procedure of re-registering as BCMP- of network.

Keywords: networks, establishments of connection in IMS, delay of transmission, analytical design, re-registering, model of alarm traffic, stream of requests, protocol of SIP, model of network of mass service, theorem of BCMP of network.

УДК 343.98 (075)

Ф.М.Мухтаров

МЕТОДЫ ЗАЩИТЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ОТ ВНЕШНИХ И ВНУТРЕННИХ ИНФОРМАЦИОННЫХ УГРОЗ

Статья посвящена классификации возможных внешних и внутренних информационных угроз и компьютерных преступлений, возникающим проблемам: стремительное наращивание процессов компьютеризации общества, ставившие врасплох правоохранительные органы, оказавшиеся неготовыми к адекватному противостоянию в борьбе с этим новым социальным явлением, а также разработки комплексных мер по обеспечению национальной безопасности.

Ключевые слова: классификация внешних, внутренних, информационных угроз, обеспечение национальной безопасности.

I. Введение

Интенсивное развитие современных телекоммуникационных сетей, активное распространение компьютерных технологий во все сферы промыш-ленности и быта, повышение доступности персональных компьютеров для любых граждан, а также широкомасштабное обучение населения навыкам программирования и использования компьютерной техники, всеобщая доступность в глобальной сети к интернет информации, к сожалению, значительно расширили возможности для совершения правонарушений в этой сфере.

Современная тенденция развития информационной системы наряду с положительными сторонами создала предпосылки для появления и негативных: появился «информационный криминал -

это действия отдельных лиц или группы лиц, направленные на взлом систем защиты, на хищение или разрушение информации в корыстных или хулиганских целях».

В мире не существует абсолютно надёжных информационных систем, гарантирующих своим пользователям полную конфиденциальность и сохранность информации, циркулирующей в них. В связи с этим возникает необходимость заниматься не только вопросами защиты средств компьютерной техники, но и решать вопросы расследования компьютерных преступлений. Однако в настоящее время в подразделениях органов внутренних дел недостаточно сотрудников, способных заниматься вопросами раскрытия компьютерных преступлений.

По мере освоения компьютеров потребителями растёт число нарушений правил информатизации, становятся более разнообразными и способы их совершения. При этом количество способов постоянно увеличивается за счёт их комбинирования.

Поэтому проблемы защиты от внешних и внутренних информационных угроз и атак не теряют своей актуальности. Это объясняется тем, что накапливаемая, хранимая и обрабатываемая в информационных системах информация является достаточно уязвимой, как с точки зрения опасности ее искажения или уничтожения нарушения физической целостности, так и с точки зрения несанкционированного доступа к ней лиц, не имеющих на это полномочий.

II. Основная часть

Анализ актуальных угроз конфиденциальной информации, на основе которого строится *система информационной безопасности предприятия* и осуществляется организация защиты информации, начинается с понимания и классификации этих угроз. В настоящий момент теория информационной безопасности рассматривает несколько классификаций информационных рисков и *угроз защиты информации*. Мы остановимся на генерализированном разделении угроз информационной безопасности интеллектуальной собственности организации на две категории – *внешние* и *внутренние* угрозы. Данная классификация предусматривает разделение угроз по локализации злоумышленника (или преступной группы), который может действовать как удалённо, пытаясь получить доступ к конфиденциальной информации предприятия при помощи сети интернет, либо же действовать посредством доступа к внутренним ресурсам IT-инфраструктуры объекта.

В случае внешних атак, преступник ищет уязвимости в информационной структуре, которые могут дать ему доступ к хранилищам данных, ключевым узлам внутренней сети, локальным компьютерам сотрудников. В этом случае злоумышленник пользуется широким арсеналом инструментов и вредоносного программного обеспечения (вирусы, трояны, компьютерные черви) для отключения систем защиты, шпионажа, копирования, фальсификации или уничтожения данных, нанесения вреда физическим объектам собственности и т.д. Внутренние угрозы подразумевают наличие одного или нескольких сотрудников предприятия, которые по злому умыслу или по неосторожности могут стать причиной утечки конфиденциальных данных или ценной информации.

Национальная безопасность – защищённость жизненно важных интересов личности, общества и государства в различных сферах жизнедеятельности от внешних и внутренних угроз, обеспечивающая устойчивое развитие страны.

Национальная безопасность - способность нации удовлетворять потребности, необходимые для ее самосохранения, самовоспроизведения и самосовершенствования с минимальным риском ущерба для базовых ценностей ее нынешнего состояния.

Национальная безопасность включает

в себя:

- государственную безопасность - понятие, характеризующее уровень защищённости государства от внешних и внутренних угроз;

- общественную безопасность – понятие, выраженное в уровне защищённости личности и общества, преимущественно, от внутренних угроз обще опасного характера;

- техногенную безопасность - уровень защищённости от угроз техногенного характера;

-экологическую безопасность и защита от угроз стихийных бедствий;

- экономическую безопасность

- энергетическую безопасность

- информационную безопасность

- безопасность личности.

Обеспечение национальной безопасности - комплекс политических, экономических, социальных, здравоохранительных, военных и правовых мероприятий, направленных на обеспечение нормальной жизнедеятельности нации, устранение возможных угроз.

Обеспечение национальной безопасности включает в себя:

- защиту государственного строя;

- защиту общественного строя;

- обеспечение территориальной неприкосновенности и суверенитета;

- обеспечение политической и экономической независимости нации;

- обеспечение здоровья нации;

- охрана общественного порядка;

- борьба с преступностью.

- обеспечение техногенной безопасности и защита от угроз стихийных бедствий.

Формирование компьютерной преступности своими корнями уходит в страны развитого капитала, поэтому необходимо использовать накопившийся зарубежный опыт в борьбе с компьютерной преступностью, экстраполируя его на отечественную почву с учётом местных особенностей.

Чем глубже какое-либо общество поражено преступным применением персональных компьютеров, тем более должны быть развиты правовые категории в области компьютерных преступлений. Интенсивный процесс компьютеризации ведёт к нарастанию и развитию различных видов компьютерных преступлений.

Существуют два основных течения научной мысли. Одна часть исследователей относит к компьютерным преступлениям действия, в которых компьютер является либо объектом, либо орудием посягательств. В этом случае кража компьютера тоже является компьютерным преступлением. Другая часть исследователей утверждает, что объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит орудием посягательства.

Компьютерных преступников можно разделить на определённые обособленные группы:

лица, в которых сочетаются профессионализм в программировании с элементами фанатизма и изобретательности. По мнению некоторых авторов, эти субъекты воспринимают средства компьютерной техники как определённый вызов своим знаниям и умениям. Здесь присутствует некий спортивный азарт. Именно это чаще всего и становится причиной преступлений. Происходит перерождение любителя-программиста в профессионального преступника;

лица, страдающие новым видом психических заболеваний-информационными болезнями или компьютерными фобиями. Эти заболевания вызывают систематическим нарушением информационного режима: информационным голодом, информационными перегрузками и т.д. Изуче-

нием данного вопроса занимается новая отрасль медицины – информационная медицина. Обычно преступления совершается ими без наличия преступного умысла. И преступлением чаще всего является повреждение или уничтожение средств компьютерной техники. При наличии подобных фактов необходимо заключение судебно-психиатрической экспертизы на предмет вменяемости преступника в момент совершения преступления. Так как во время совершения преступления происходит в какой-то степени потеря контроля над своими действиями;

профессиональные компьютерные преступники. Здесь присутствуют явно корыстные цели. Преступники данной группы чаще всего входят в состав каких-нибудь преступных образований. Это высококлассные специалисты, которые представляют явную угрозу для общества. Последних можно разделить еще на две группы по категориям доступа к средствам компьютерной техники;

внутренние пользователи (лица, которые имеют непосредственный доступ к необходимой информации);

внешние пользователи (субъекты, которые обращаются к информационной системе или посреднику за получением необходимой им информации).

По мнению специалистов, подавляющее число преступлений совершается именно внутренними пользователями (обычно это рабочие и служащие фирм и компаний). Внешние пользователи - это лица, которые хорошо осведомлены о деятельности потерпевшей стороны. Круг внешних пользователей настолько широк, что не поддается никакой систематизации и классификации (ими может быть практически любой человек).

Для *защиты от внешних угроз* информационной безопасности отлично зарекомендовали себя системы предотвращения вторжений на уровне хоста (HIPS). Правильно настроенная система даёт беспрецедентный уровень защищённости, близкий к 100%. Грамотно выработанная политика безопасности, применение совместно с HIPS других программных средств защиты информации (например, антивирусного пакета) предоставляют очень высокий уровень безопасности. Организация получает защиту практически от всех типов вредоносного ПО, значительно затрудняет работу хакера, решившего попробовать пробить информационную защиту предприятия, сохраняет интеллектуальную собственность и важные данные организации.

Защита от внутренних угроз также требует комплексного подхода. Он выражается в выработке должных политик информационной безопасности, введением чёткой организационной структуры ответственных за информационную безопасность сотрудников, контроле документооборота, контроле и мониторинге пользователей, введении продвинутых механизмов аутентификации для доступа к информации разной степени важности. Степень такой защиты зависит от объективных потребностей организации в защите информации. Далеко не всем объектам требуется дорогостоящая DLP-система, дающая неплохие результаты по *защите данных предприятия* от утечек, но требующая сложнейшей процедуры внедрения и пересмотра текущих механизмов документооборота. Оптимальным выбором для большинства компаний станет введение функционала защиты от утечек данных, контроле документооборота и мониторинг действий пользователей локальной сети организации. Такое решение является недорогим, простым в развёртывании и эксплуатации, но весьма

эффективным инструментом информационной безопасности.

Проблемы обеспечения безопасности информации в информационных сетях, как объектах, наиболее часто подвергающихся нападению, за счет интенсивного расширения числа абонентов сети дало возможность увеличения, уязвимости систем за счет использования в узлах сети персональных компьютеров. Это в свою очередь дало в руки злоумышленникам уникальный по своим возможностям инструмент разведки и проникновения в сеть. В связи с этим стали разрабатываться определенные механизмы, с помощью которых обеспечивалась защита информации. Здесь под защитой информации следует понимать процесс создания и использования в информационных системах специальных механизмов, поддерживающих установленный статус ее защищенности.

В зависимости от местонахождения источника возможной угрозы, все угрозы разделяют на две группы: внешние и внутренние. К внешним угрозам информационной безопасности относятся:

- деятельность иностранных разведывательных и специальных служб;

- деятельность конкурирующих иностранных экономических структур;

- деятельность политических и экономических структур, преступных групп и формирований, а также отдельных лиц внутри страны, направленная против интересов граждан, государств и общества в целом и проявляющаяся в виде воздействий на информационный сеть;

- стихийные бедствия и катастрофы.

К внутренним угрозам информационной базы относятся:

- нарушения установленных требований информационных баз, допускаемые обслуживающим персоналом и пользователями информационной системы;

- отказы и неисправности технических средств обработки, хранения и передачи сообщений, средств защиты и контроля эффективности, принятых мер по защите, сбои программного обеспечения, программных средств защиты информации и программных средств контроля эффективности принятия мер по защите.

Угроз информации можно разделить на: информационные, программно-математические, физические и организационные. Информационные угрозы проявляются в виде:

- нарушения адресности и своевременности информационного обмена, противозаконного сбора и использования информации;

- осуществления несанкционированного доступа к информационным ресурсам и их противоправного использования;

- хищения информационных ресурсов из банков и баз данных;

- нарушения технологии обработки информации. Программно-математические имеют следующие виды:

- внедрения в аппаратные и программные изделия компонентов, реализующих функции, не описанные в документации на эти изделия;

- разработки и распределения программ, нарушающих нормального функционирования информационных систем или их систем защиты информации.

К физическим угрозам относятся:

- уничтожения, повреждения, радиоэлектронного подавления или разрушения средств и систем обработки информации, телекоммуникации связи;

- хищение программных или аппаратных ключей и средств криптографической защиты информации;

- перехвата информации в технических каналах связи и телекоммуникационных системах;

- внедрение электронных устройств перехвата информации в технические средства связи и телекоммуникационные системы, а также в служебные помещения;

- перехвата, дешифрования и навязывания ложной информации в сетях пере-

дачи данных и линиях связи;

- воздействия на парольно-ключевые системы защиты средств обработки и передачи информации.

Организационные угрозы состоит из:

- невыполнения требований законодательства в информационной сфере;
- несанкционированный доступ к информационным ресурсам;
- манипулирование информацией (дезинформация, скрытие или искажение информации);
- несанкционированное копирование данных;
- хищение ценных информации из баз данных и банков данных;
- хищение носителей информации;
- уничтожение или модификация данных;
- противоправной закупки несовершенных или устаревших информационных технологий, средств информатизации, телекоммуникации и связи.

Относительная новизна возникших проблем, стремительное, наращивание процессов компьютеризации общества застали врасплох правоохранительные органы, оказавшиеся неготовыми к адекватному противостоянию и активной борьбе с этим новым социальным явлением.

Резюмируя выше сказанные можно сделать вывод о том, что следователи, производящие расследование компьютерных преступлений, сталкиваются со многими, подчас неразрешимыми трудностями, среди которых представляется возможным выделить следующие:

- сложность квалификации преступных деяний;
- сложность в проведении различных следственных действий из-за несовершенства действующего уголовно-процессуального законодательства;
- сложность в назначении программно-технической экспертизы средств компьютерной техники и в формулировке вопросов, выносимых на рассмотрение эксперта;
- отсутствие по некоторым вопросам соответствующих специалистов, необходимых для привлечения в ходе следствия;
- отсутствие элементарных познаний в области компьютерной техники т.д..

Большинство специалисты, затрудняет процесс расследования компьютерных преступлений такое обстоятельство, как сокрытие преступникам следов своей деятельности, например, путём стирания данных или путём введения в компьютерную систему потерпевшей стороны вредоносных программ. Непросто также установить причинно-следственную связь между фактом совершения преступления и подозреваемым, особенно в случае наличия значительного числа пользователей компьютерной системы.

III. Заключение.

В настоящее время имеется немало возможностей, способствующих раскрытию компьютерных преступлений. Однако их эффективность зависит от ряда объективных и субъективных обстоятельств, из которых на первое место выступает создание в системе правоохранительных органов общего организационно-методического центра, координирующего всю работу в этом направлении, наделённого соответствующими полномочиями и способного по своему профессиональному составу заниматься всем спектрам проблем, связанных с компьютерной преступностью.

Литература

1. Мухтаров Ф.М., Шкляровский Б.А.. “Предпосылки обеспечение конфиденциальности информационных ресурсов в электронном правительстве”, Сборник докладов республиканской научно-технический конференции “Значение информационно-коммуникационных технологий в инновационном развитии реальных отраслей экономики” часть 1 , г.Ташкент, 6-7 апреля 2017 г., ТУИТ, 23-25 стр..

2. Мухтаров Ф.М., Ташмухамедова Д.К.

"Обеспечение конфиденциальности информационных ресурсов в электронном правительстве", ФерПИ научно–технической журнал, г.Фергана, 2018 г. 22-том №1 216-218 стр.

3. Якубов М.С., Левченко Э.П. Проблемы обеспечения информационной безопасности // Ж. Хукук.-2002.-№ 3 (5).-Т.: МВД Республики Узбекистан. С. 50-54 стр.

Mukhtarov Farrukh Mukhammadovich.
The independent employee the scientific researcher, the Tashkent university of information technologies of Muhamed al-Khwarizmi.
E mail: fmm1980@rambler.ru

Mukhtarov F.M.

Methods of protection of national security from external and internal information threats

The article is devoted to classification of possible external and internal information threats and computer crimes, the arising problems: the prompt strengthening of processes of a computerization of society, the law enforcement agencies putting unawares which were not ready to adequate opposition in fight against this new social phenomenon and also development of complex measures for ensuring national security.
Keywords: categorization, external, internal, information threats, provision of national safety.

UDC 004.942

Sh.B.Redjepov, S.Uguz

TRANSITION RULES OF LINEAR CELLULAR AUTOMATA OVER BINARY FIELD AND IMAGE ANALYSIS

This paper investigates the theoretical aspects of two-dimensional (2D) linear cellular automata (CA) over binary field combining with image science application. The present study focuses on the theory of 2D linear CA with respect to uniform null and adiabatic boundary CA conditions. It is considered geometrical and visual aspects of patterns generated by these CA evolution. Multiple copies of any arbitrary seed image corresponding to CA could be obtained by using the transition rules of these CAs. Also we believe that these type of CA could be found many different applications in special case situation e.g. computability theory, mathematics, theoretical biology, DNA genetics research, image science, textile design, video processing and microstructure modeling., etc. in near future.
Keywords: Cellular automata, null and adiabatic boundary, CA and Image analisys.

Introduction

Cellular automata (CAs for brevity) introduced by Ulam and von Neumann [1] in the early 1950's, have been systematically studied by Hedlund from purely mathematical point of view. One-dimensional CA has been investigated to a large extent. However, little interest has been given to two-dimensional cellular automata (2D CA). Von Neumann [1] showed that a cellular automaton can be universal. Due to its complexity, von Neumann rules were never implemented on a computer. In the beginning of the eighties, Wolfram [2] has studied in much detail a family of simple one-dimensional (1D) CA rules and showed that even these simplest rules are capable of emulating complex behavior. Some basic and precise mathematical models using matrix algebra over the binary field which characterize the behavior of 2D nearest neighborhood linear CA with null and periodic boundary conditions have been seen in the literature [3, 7, 8, 9, 10, 11]. CA has received remarkable attention in the last few decades [11, 12, 13, 14, 15, 16]. Due to its structure CA has given the opportunity to model and understand many behaviors in nature easier. Most of the work for CA is done for one-dimensional (1D) case. The paper [14] deals with the behavior of the uniform 2D CA over binary fields.

Here we study the theory of 2-dimensional uniform null and adiabatic boundary CA (2D NB CA, 2D AB CA) of the all linear rules (e.g. von Neumann, Moore neighborhood and the others) and applications of image