construction of such approximations from known subspaces acceptable for defined Boolean function. We show that the proposed algorithm allows us to construct much more efficient attacks on synchronous stream ciphers compared with exhaustive search.
Index Terms: stream cipher, non-linear cryptanalysis, chosen IV attack, algebraic degenerate function, finding approximations of Boolean functions.

Олексійчук Антон Миколайович, доктор технічних наук, професор Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ».
E-mail: alex-dtn@ukr.net.
Алексейчук Антон Николаевич, доктор технических наук, профессор Института специальной связи и защиты информации НТУУ «КПИ».
Alekseychuk Anton, Doctor of Technical Science, Professor of Institute of Special Communication and Information Security of NTUU «KPI».

Конюшок Сергій Миколайович, кандидат технічних наук, доцент, заступник начальника Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ».
E-mail: 3tooth@mail.ru.
Конюшок Сергей Николаевич, кандидат технических наук, доцент, заместитель начальника Института специальной связи и защиты информации НТУУ «КПИ».
Konyushok Sergey, Candidate of Technical Science, docent, vice-head of Institute of Special Communication and Information Security of NTUU «KPI».

Сторожук Артем Юрійович, аспірант Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ».
E-mail: storojs72@gmail.com.
Сторожук Артем Юрьевич, аспирант Института специальной связи и защиты информации НТУУ «КПИ».
Storozhuk Artem, post-graduate student of Institute of Special Communication and Information Security of NTUU «KPI».

УДК 004.056.53:004.492.3 (045)

ЗАЩИТА АВИАЦИОННЫХ БОРТОВЫХ СЕТЕЙ ОТ АТАК МЕТОДАМИ ТЕОРИИ КОНФЛИКТА С ПРИМЕНЕНИЕМ МЕДОВЫХ ЛОВУШЕК

Сергей Водопьянов, Владимир Дрововозов, Елена Толстикова

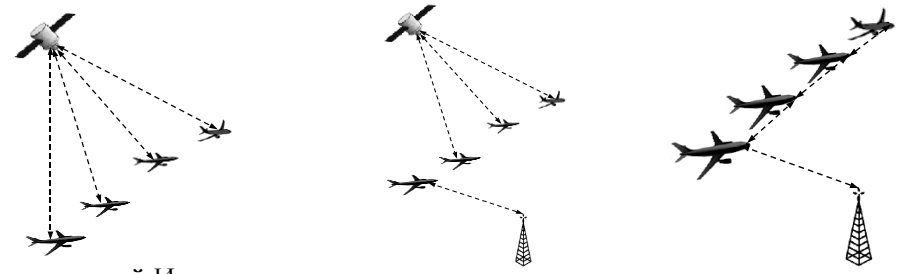
Проблема защиты авиационных бортовых сетей от несанкционированных вторжений стоит особенно остро в связи с необходимостью безусловного обеспечения безопасности полетов, исключения летных происшествий и предпосылок к ним. Для защиты сети от внешних и внутренних атак необходимо не просто повышать энергетические и информационные ресурсы, а применять оптимальные методы борьбы с разумным противником. В работе предложены математические модели конфликтного взаимодействия с применением "медовых ловушек" – псевдосервисов, затягивающих противника в эскалацию атаки, вынуждающую его расходовать свои энергетические и информационные ресурсы. Разработана концептуальная модель построения комбинированной системы защиты с внедренным дополнительным уровнем защиты – сетевой медовой ловушки. Проведено компьютерное моделирование, результаты которого свидетельствуют о высокой эффективности разработанного метода защиты сети.
***Ключевые слова**: авиационная бортовая сеть, теория конфликта, медовая ловушка, марковский процесс, альтернирующий процесс восстановления.*

Введение. Мобильные коммуникации и организация доступа к Интернету для доступа к данным становятся все более востребованными в современных и тем более в будущих авиационных системах *CNS/ATM*. На первых этапах развития авиационных бортовых сетевых структур основное внимание уделялось использованию спутниковых коммуникационных систем и глобальных компьютерных сетей на их базе [1]. При выполнении полетов большой протяженности, включая трансконтинентальные полеты, а также полеты над пустынями, в полярных регионах, спутниковые коммуникационные системы играют основную роль в организации и развертывании глобальной авиационной сетевой инфраструктуры.

В настоящее время активно внедряются локальные компьютерные сети разного масштаба типа сотовых информационно-коммуникационных и вычислительных систем с самоорганизацией. Они имеют смешанную структуру "борт – борт" или "борт – земля". Благодаря таким системам обеспечиваются быстрый и экономичный

доступ на протяжении полетов средней и малой протяжности.

Процесс эволюции авиационных информационно-коммуникационных и вычислительных сетей напоминает соответствующий процесс эволюции наземных компьютерных сетей [2]: от глобальных сетей типа *ARPANET* к сетям масштаба мегаполиса *MAN* или крупной корпорации и локальным сетям *LAN*. На рис. 1 схематически изображен процесс эволюции подходов к общей организации и аппаратной реализации авиационных сетей – от а) исключительно спутниковых каналов доставки данных к б) смешанным системам и в) автономным локальным сетям.



а) спутниковый Интернет б) смешанный доступ в) локальная сеть

Рис. 1. Этапы развития авиационных сетей: от спутникового Интернета до локальных сетей доступа "борт – земля"

Переход от исключительно спутниковых коммуникационных систем к смешанным и автономным сетевым системам обусловлен, в том числе, и желанием обеспечить непрерывный доступ к источникам информации и снизить задержки доставки, особенно в нештатных ситуациях. При работе со спутниками, которые находятся на геостационарных орбитах, задержка доставки, даже без учета задержек при обработке в сетевых коммутационных узлах, составляет около 250 мс. С другой стороны, низкоорбитальные спутники не всегда могут обеспечить непрерывную доставку данных к пользователям.

Одним из краеугольных камней усовершенствования авиационной коммуникационной инфраструктуры является бесшовная организация авиационных сетей и стыковка сетевых сегментов [3]. Если рассматривать аэроузел как автономный элемент авиатранспортной инфраструктуры, то одним из важнейших автономных сетевых сегментов аэроузла, соответственно, является авиационная сеть с мобильными узлами. Рассмотрим ее типовую структуру и параметры. На рис. 2 изображена типичная схема организации авиационной бортовой сети для обмена данными по направлениям "борт – борт" и "борт – земля". Соответственно, на рис. 3 изображена схема сети, в которую входят мобильные сетевые узлы – маршрутизаторы и/или программные коммутаторы (Softswitch). Последние могут быть заменены системами класса IMS – IP Multimedia Subsystem, но только для "чистых" IP-сетей с соответствующей инфраструктурой. Кроме того, технология Softswitch является хорошо отработанной, и как любая зрелая технология, нуждается лишь в доработке практических вопросов – обеспечение безопасности, взаимодействия с новыми сетевыми технологиями, оптимизации параметров функционирования и т.п.

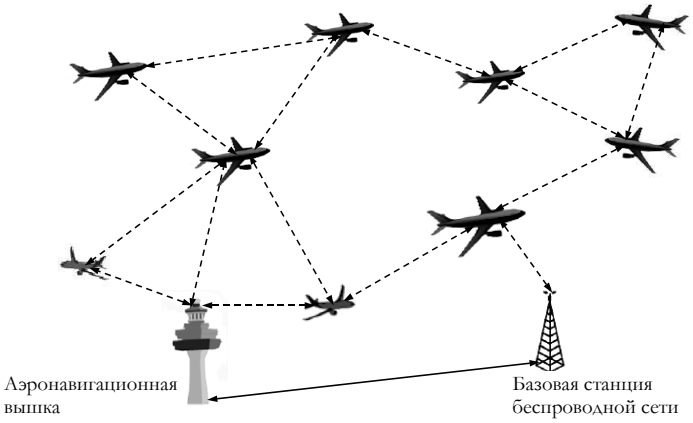


Рис. 2. Схема применения авиационной бортовой сети для обмена данными по каналам "борт – борт" и "борт – земля"

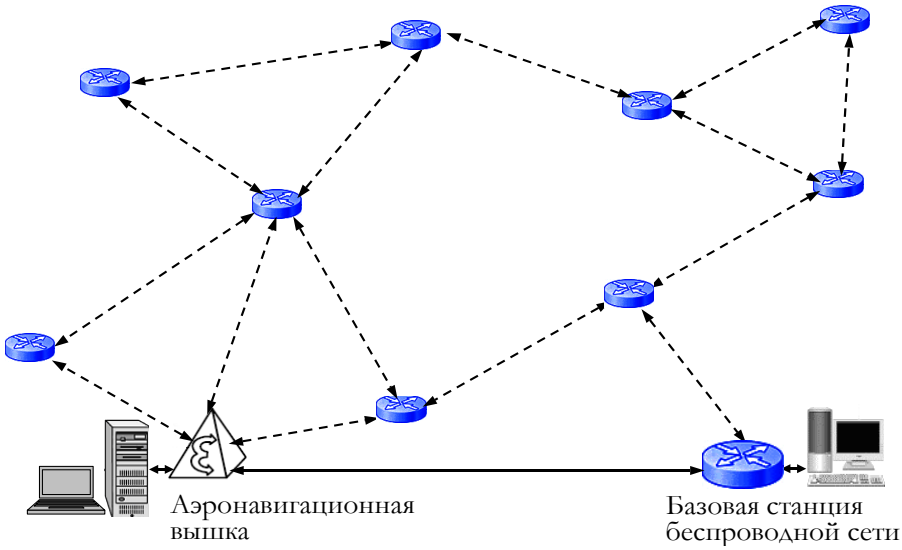


Рис. 3. Пример текущей топологии авиационной бортовой сети

Одной из основных проблем организации и функционирования авиационных бортовых сетей является обеспечение их безопасности и защиты информации, циркулирующей в сети. Поскольку авиационные бортовые сети в принципе могут быть только беспроводными, их уязвимость к несанкционированному доступу (вторжениям) является достаточно высокой. При этом угрозы могут быть как внешними, так и внутренними – от пассажиров, находящихся на борту воздушного судна (ВС) и получающих сервисную и медийную информацию через интерфейсы общего доступа [4].

Для защиты от угроз разного вида традиционные подходы к безопасности необходимо дополнять системами обнаружения атак, работающими на основе косвенных признаков (поведение внешних и внутренних пользователей) и статистического анализа (корреляции) событий. Преимущество таких систем в том, что они способны противостоять не только известным, но и новым угрозам.

Одним из таких средств, позволяющих значительно повысить безопасность информационной сети, являются honeypot-системы [5]. Honeypot имитирует работу реальной системы, являющейся потенциальной целью атак и несанкционированного доступа, отвлекает на себя внимание и ресурсы нарушителя, фиксирует все его действия и информирует оператора сети о фактах нарушений. В зависимости от типа honeypot имитироваться могут любые системы, служащие потенциальными объектами для атак: серверы, базы данных, сетевые сервисы, файловые ресурсы и т.д.

Преимущества honeypot-систем определяются самим принципом их работы. Поскольку honeypot лишь имитирует реальную систему, и к нему не обращаются ни реальные пользователи сети, ни легальные сетевые приложения, то любая активность на honeypot и любая попытка обращения к нему является несанкционированной и свидетельствует либо об атаке, либо об исследовании сети с целью найти уязвимые места в ее защите. Отсюда следует и еще одно преимущество – обнаружение новых типов атак, так как активность на ловушке регистрируется независимо от типа атаки.

Цель работы. Целью исследований является рассмотрение вопросов организации системы защиты информационной сети и построение математических моделей процессов защиты. Вполне логично использовать для защиты все сетевые ресурсы с применением honeypot-ловушек [6] путем создания распределенной honeypot-системы – так называемой сети honey net. При этом сеть honey net используется как дополнительное средство защиты совместно с межсетевым экраном (Firewall) и системой обнаружения вторжений (Intrusion Detection System – IDS).

Постановка и решение задачи. Принципиальной особенностью сети с мобильными узлами является ее переменная структура. Вследствие перемещения летательных аппаратов (ЛА) в зоне аэроузла текущая топология и количество сетевых элементов непрерывно меняются: одни ЛА входят в зону ответственности аэроузла, другие, наоборот, из нее выходят. Процесс изменения топологии и структуры бортовой авиационной сети представим в виде процесса "гибели и размножения" [7]. Событие появления нового сетевого узла рассматривается как размножение, выход узла из зоны покрытия сети – как гибель. Кроме того, примем предположение о том, что

вероятность одновременной смены двух и более узлов – величина второго порядка малости и здесь не рассматривается.

Метод медовой ловушки – заманивания на ложные информационные объекты, обладающие высокой уязвимостью – по существу, можно отнести к методам теории конфликта [8], в частности, к методу затягивания в эскалационную воронку [9]. Противник, обнаружив уязвимость информационного объекта, увеличивает свою активность. Для провоцирования противника на сосредоточение своих ресурсов в этом направлении объект атаки сначала демонстрирует уверенность – продолжает работать с применением простых решений, несмотря на противодействие и атаки. После такой демонстрации противник может начать повышать атакующий ресурс и, в конце концов, уйти с ложного информационного объекта. Чтобы удержать противника на этом объекте, целесообразно демонстрировать растерянность: беспорядочную смену мер защиты и режимов работы защищаемого объекта.

Такая смена режимов работы (рефлексивное управление) позволит затягивать противника в эскалацию атаки и удерживать на ложном информационном объекте. Процесс затягивания в эскалационную воронку (медовую ловушку honeypot, медовую сеть honey net) можно рассматривать как альтернирующий процесс восстановления [7].

С учетом изложенного сформулируем задачу исследования – разработать метод управления процессом защиты авиационной бортовой сети на основе теории конфликта и управляемых марковских процессов [10].

Рассмотрим математические модели процесса гибели и размножения и альтернирующего процесса восстановления применительно к конкретной рассматриваемой задаче.

Пусть авиационная бортовая сеть (в дальнейшем – сеть) в каждый момент времени может находиться в одном из состояний $s_0, s_1, s_2, \ldots, s_N$. Текущее количество ЛА в зоне и, соответственно, число узлов сети численно равны номеру состояния. N – максимально допустимое по соображениям безопасности полетов число ЛА в зоне. За промежуток времени $[t, t+\tau]$ число ЛА может увеличиться или уменьшиться на единицу, т.е. сеть из состояния s_k может перейти в состояние s_{k+1} с вероятностью $\lambda_k\tau$ или в состояние s_{k-1} с вероятностью $\mu_k\tau$. λ_k и μ_k – интенсивности переходов на интервале времени τ. Вероятность сохранения прежнего состояния равна $1-(\lambda_k+\mu_k)\tau$. Считаем, что вероятности переходов на интервале времени τ из состояния s_k в состояние s_{k+m} или в состояние s_{k-m}, $m \geq 1$ являются величинами второго порядка малости по сравнению с $\lambda_k\tau$, $\mu_k\tau$. В общем случае λ_k и μ_k зависят от k и t.

Пусть в момент t сеть находится в состоянии s_k. Обозначим вероятность этого события через $p_k(t)$. Тогда при $k=1$

$$\frac{dp_0(t)}{dt} = -\lambda p_0(t) + \mu_1(t), \qquad (1)$$

а при $k \geq 1$

$$\frac{dp_k(t)}{dt} = -(\lambda_0+\mu_k)\,p_k(t) + \lambda_{k-1}p_{k-1}(t) + \mu_{k+1}p_{k+1}(t). \qquad (2)$$

Поскольку число состояний (количество узлов сети) ограничено, полученные уравнения представляют собой частный случай классических уравнений А.Н. Колмогорова, которыми управляется стохастически непрерывный марковский процесс [7]. Здесь основной характеристикой состояния сети является вероятность переполнения зоны полетов ЛА. Эта вероятность вычисляется по формулам Эрланга при любом распределении длительности нахождения ЛА в зоне.

Для построения математической модели процесса противодействия вторжению рассмотрим две взаимно независимые последовательности случайных величин:

– первого вида $\{\tau_1', \tau_2', \tau_3', \ldots\}$ – последовательность попыток вторжения в сеть;

– второго вида $\{\tau_1'', \tau_2'', \tau_3'', \ldots\}$ – последовательность действий по противодействию вторжениям.

Процесс начинается с интервала τ_1' первого вида, в конце которого имеет место событие первого вида. За ним следует интервал τ_1'' второго вида, заканчивающийся событием второго вида в момент времени $\tau_1' + \tau_1''$, после чего процессы циклически повторяются; $(2k-1)$-е событие первого вида происходит в момент времени $\tau_1' + \ldots + \tau_k' + \tau_1'' + \ldots \tau_{k-1}''$, а $2k$-е событие второго вида, осуществляется в момент времени $\tau_1' + \ldots + \tau_k' + \tau_1'' + \ldots \tau_k''$. Получающийся случайный точечный процесс с поочередными интервалами двух видов называется альтернирующим процессом восстановления (см. рис. 4).

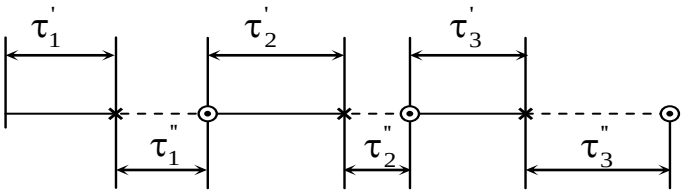


Рис. 4. Альтернирующий процесс восстановления
(— интервал I вида; - - - интервал II вида; × – событие I вида; ⊙– событие II вида).

При теоретическом рассмотрении альтернирующих процессов восстановления обычно полагают, что смена состояний (типов интервалов) описывается цепью Маркова с двумя состояниями и с известной матрицей перехода, т.е., по существу, полумарковским процессом.

Если последовательность моментов $\left[\tau_k^{'}, \tau_k^{''}\right]$ образована независимыми неотрицательными величинами с распределениями $\left[F_k'(x),\ F_k''(x)\right]$, то для стационарных процессов восстановления эти распределения должны быть одинаковы при всех $k \geq 1$. Кроме того, по определению λ – параметра потока и с учетом ординарности потока $F_k'(\tau) = \lambda_k^{'}\tau_k^{'};\ \ F_k''(x) = \lambda_k^{''}\tau_k^{''}$.

Отметим, что при весьма широких условиях относительно исходных потоков, имеющих место в отдельных сетевых узлах, суммарные потоки будут близки к пуассоновским, в том числе и к простейшим.

Рассмотрим теперь структуру системы защиты.

Многоуровневая система защиты авиационной бортовой сети

Процедуры выбора и сравнительного анализа эффективности той или иной стратегии защиты, как правило выбираются на основе суждений экспертов. Как всякая процедура метода экспертных оценок, они несут на себе отпечаток субъективизма. Поэтому рассмотрим ограниченный набор наиболее наглядных стратегий защиты:

– эшелонирование рубежей защиты типа "внешняя – демилитаризованная – внутренняя зоны безопасности";

– отказ от получения – простой возврат подозрительного трафика;

– распределенный отказ от получения – трансляция подозрительного трафика на сетевые узлы и возврат источнику со всех этих точек;

– насыщение рубежей защиты псевдосервисами с воспроизведением хорошо известных уязвимостей – затягивание противника в эскалационную ловушку.

Для обеспечения эффективной фиксации действий нарушителей необходимо использовать несколько различных уровней сбора данных [5, 6].

Первый уровень — это шлюз на границе периметра защищаемой сети. Сетевые пакеты на данном уровне могут отслеживаться с использованием межсетевого экрана (МЭ) и системы обнаружения вторжений (СОВ). Здесь просматривается весь сетевой трафик, который поступает в сеть, идентифицируются и блокируются удаленные атаки.

Второй уровень сбора данных — это журнал регистрации мостового (граничного) компонента второго уровня, реализуемого, например, на основе использования МЭ или СОВ. Этот компонент должен иметь механизм фильтрации и модификации пакетов, позволяющий блокировать исходящие соединения при обнаружении определенной сигнатуры (например, достижении установленного предельного числа исходящих соединений) и (или) изменять содержимое сетевых пакетов, обезвреживая атаки.

Третий уровень предназначен для сбора информации о деятельности нарушителя в системе, в том числе о командах, инициированных нарушителем. Нарушители, чтобы скрыть свои действия, могут использовать шифрование. Например, как только нарушитель проник на хост, он может осуществлять удаленное администрирование системы с помощью SSH. Для решения этой проблемы можно использовать специальные модули ядра ОС. Эти модули накапливают информацию обо всей деятельности нарушителей. Информацию, которую собирают модули ядра, нельзя сохранять локально, поскольку нарушитель может обнаружить и удалить или изменить эту информацию. Поэтому указанную информацию необходимо удаленно собирать на защищенной системе, причем так, чтобы нарушитель об этом не знал. Это должна делать СОВ компонента второго уровня. Она действует как сетевой анализатор, накапливающий сведения и регистрирующий всю деятельность нарушителей, записывая, в том числе, все пакеты, сгенерированные модулями ядра.

Цель контроля данных – снижение риска использования ловушек. Эта задача может быть выполнена с помощью дополнительного мостового (граничного) компонента Honey Net, реали-

зуемого, например, на основе использования МЭ или СОВ. Этот компонент реализует фильтрацию и модификацию исходящих сетевых пакетов, обеспечивая блокировку исходящих соединений при обнаружении определенной сигнатуры и (или) изменение содержимого сетевых пакетов для обезвреживания атак.

На рис. 5 изображена концептуальная схема сетевой защиты с применением функций "медовой ловушки".

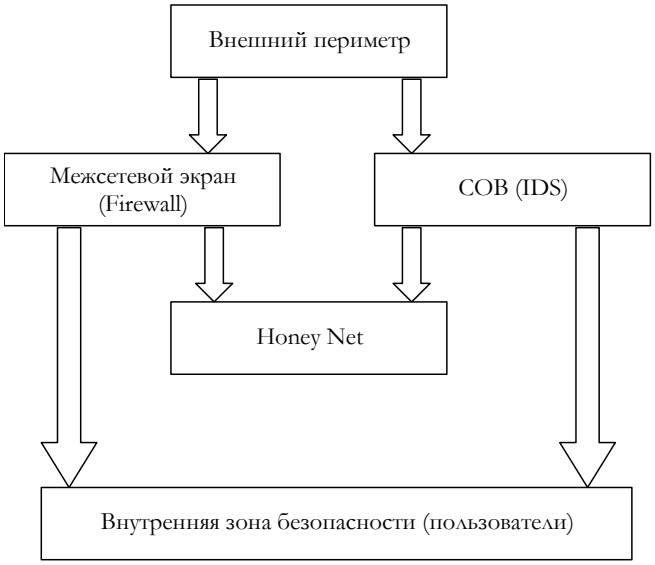


Рис. 5. Концептуальная модель сетевой защиты

Сеть Honey Net выполняет функции ловушки и терминирования подозрительного трафика. Например, наиболее вероятными троянским программами, атакующими порт 80, являются Back End, Executer, Hooker, RingZero. Для альтернативного порта 8080 – RingZero. В целом в качестве вектора управления рассматривается набор управляющих воздействий на порты сетевых узлов. Защита начинается с определения используемых портов и закрытия остальных в штатном режиме. На сетевом узле выделяются следующие роли, которые он исполняет: Web-сервер (порты 80 и, возможно, 8080 в качестве альтернативного), почтовый сервер (SMTP и POP3 протоколы – 25 и 110-й порты). Добавим еще по 2 порта для DHCP и DNS служб. Также для удаленного подключения по SSH используется один порт. Часто используются порты для шифрованного подключения через http – https (еще 2 порта). Таким образом, уже имеем 9 портов, необходимых для работы. Если добавить еще несколько сопутствующих служб, запущенных на сервере, то количество портов может увеличиться до нескольких десятков. Остальные, не нужные для работы в штатном режиме порты должны быть закрыты.

В режиме атаки открываются псевдосервисы и закрываются реальные сервисы, которые подвергаются атаке (например, Web-сервер). Меняются значения соответствующих компонентов (управляющих сигналов).

Результаты моделирования системы защиты на основе Honey Net

С использованием математической модели конфликта между распределенными системами атаки и защиты разработана программа компьютерного моделирования атакующих и контратакующих потоков. Имеют место последовательности атакующих действий и ответных защитных мер (пассивных, активных или и тех, и других). Предположим, что в результате атаки вероятность штатного функционирования объекта снижается, возможно, до нуля, а в результате применения ответной защитной меры вероятность функционирования объекта повышается, возможно, вплоть до исходной величины. Процесс развития конфликта представляет собой полумарковский процесс типа альтернирующего процесса восстановления, переходные и финальные вероятности которого зависят от соотношения стратегических (S_{ids}, S_{icm}) и энергоинформационных (E_{ids}, E_{icm}) ресурсов сторон [9].

Исходные данные (весовые функции, коэффициенты) в основном выбирались с точностью до порядка величины. Учитывая высокую степень априорной неопределенности, широкий диапазон случайных мешающих воздействий, можно считать такой выбор приемлемым для получения оценочных характеристик процесса развития конфликта и финальных (асимптотических) оценок.

На приведенных ниже рисунках изображены графики изменения относительного выигрыша защищающейся стороны в конфликте:

– на рис. 6 – ресурсы защиты больше ресурсов атакующей стороны в два раза;

– на рис. 7 – ресурсы защиты меньше ресурсов атакующей стороны в три раза.

По оси абсцисс отложены интервалы обмена трафиком между атакующей и защищающейся сторонами. Единичному интервалу соответствует в среднем сто получаемых и отправляемых информационных посылок.

Численные характеристики выигрыша (проигрыша) оцениваются вероятностью снижения качества сервиса QoS в процессе отражения атаки. Считается, что эта вероятность распределена по Гауссовскому закону с нулевым математическим ожиданием и единичной дисперсией.

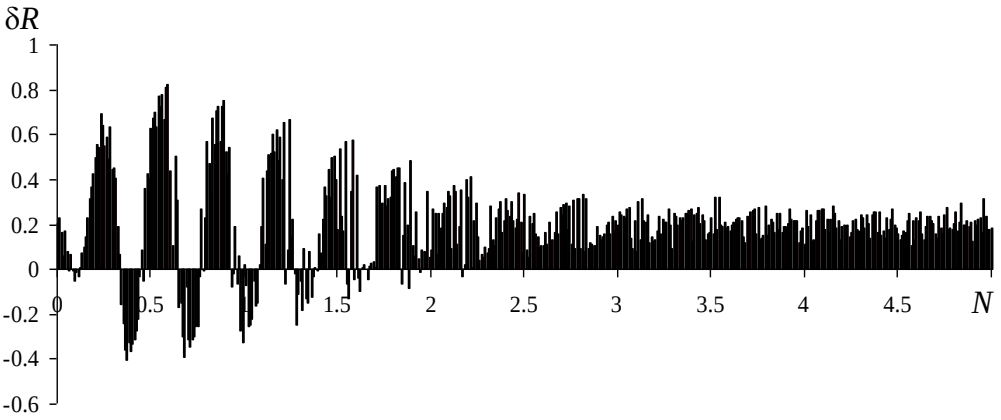


Рис. 6. Ресурсы защиты выше в два раза. Выигрыш в конфликте. $P_{QoS} \approx 0,02$

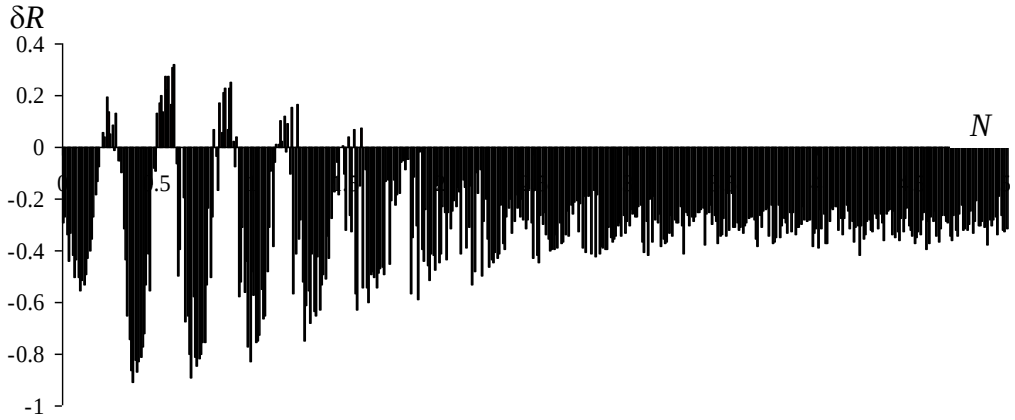


Рис. 7. Ресурсы защиты ниже в три раза. Проигрыш. $P_{QoS} \approx 0,88$

На рис. 8 изображен график выигрыша при попадании противника на псевдосервис. В данном случае порт 80 закрывался, а в качестве псевдосервиса использовался альтернативный порт 8080. Тогда противник направлял атакующие воздействия на этот порт, где они просто терминировались.

Видно, что при ресурсе защиты, в три раза меньшем ресурса атаки, имеет место нулевой выигрыш и, соответственно, $P_{QoS} \approx 0,5$ (ср. с результатами, приведенными на рис. 7).

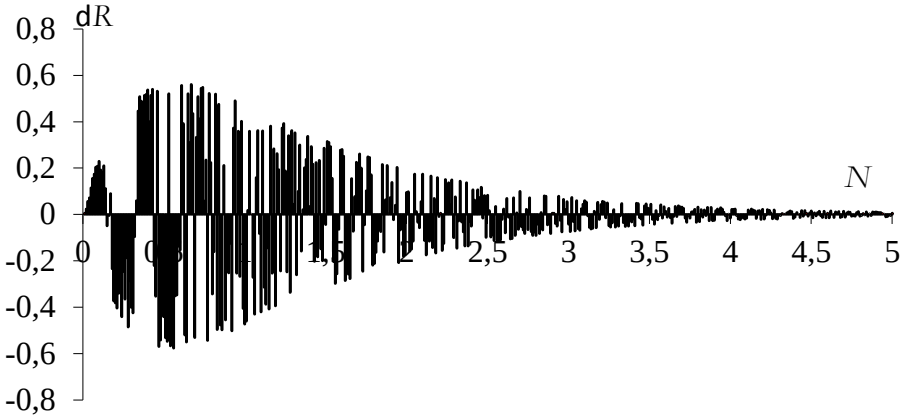


Рис. 8. Ресурсы защиты ниже в три раза. Включение псевдосервиса (открытие альтернативного порта для терминирования атакующих воздействий) в точке 221. $P_{QoS} \approx 0,5$

Результаты моделирования свидетельствуют о том, что выигрыш зависит не только от соотношения ресурсов сторон конфликта, но и от эффективности выбранной стратегии. Затягивание противника в процесс атаки ложных объектов выгоднее простого наращивания своего энергоинформационного ресурса.

Выводы. Специфика авиационных бортовых сетей заключается в непрерывном изменении структуры и состава пользователей сети и в по-

вышенных требованиях к защите от внешних и внутренних злоумышленников.

При использовании методов конфликтного управления процессами защиты компьютерных сетей можно добиваться выигрыша, даже если противник имеет заметное превосходство в ресурсах. Решение этой задачи достигается путем рефлексивного управления – учета сильных и слабых сторон противника, целенаправленного истощения его ресурсов в атаках на ложные объекты и псевдосервисы.

В дальнейшем планируется провести исследования динамики изменения сетевых структур и влияния этих изменений на эффективность систем защиты на основе honeypots и Honey Nets как систем с переменной структурой.

ЛИТЕРАТУРА

[1]. Future Aeronautical Communications / Edited by Simon Plass. – Institute of Communications and Navigation, German Aerospace Center (DLR), Germany. – Published by InTech Janeza Trdine 9, 51000 Rijeka, Croatia. – InTech, 2011. – 378 PP.

[2]. Tanenbaum, A.S. Computer Networks, 5th Ed. / Andrew S. Tanenbaum, David J. Wetherall. – Prentice Hall, Cloth, 2011. – 960 PP.

[3]. Vodopianov S. Optimisation of Network Structures of Air Traffic Control Systems / Proceedings of the 6th International Conference "Advanced Computer Systems and Networks: Design an Application" – ACSN-2013. – Sept. 16 – 18, 2013. – Lviv, Ukraine. – PP. 84 – 85.

[4]. Airlines Electronic Engineering Committee (AEEC). ARINC Report 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework, December 2005.

[5]. Mohd. Junedul Haque. An Approach for Intrusion Detection using HoneyPots to Improve Network Security // International Journal for Research in Applied Science & Engineering Technology (IJRASET). – Volume 3 Issue IV, April 2015. – pp. 1029 – 1033.

[6]. Lenny Zeltser. Experimenting with Honeypots Using The Modern Honey Network 20 Feb 2015. – Электронный ресурс. Режим доступа: https:// zeltser.com/modern-honey-network-experiments/

[7]. Тихонов В.И., Миронов М.А. Марковские процессы. М.: Советское радио, 1977. – 488 с.

[8]. Дружинин В.В., Конторов Д.С., Конторов М.Д. Введение в теорию конфликта. – М.: Радио и связь, 1989. – 288 с.

[9]. Виноградов Н. А., Данилина Г. В., Домарев Д. В., Милокум Я. В.Управление псевдосервисами в защищенных информационных системах на основе теории конфликта //Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – №6(34). – с. 5-12.

[10]. Дынкин Е.Б., Юшкевич А.А. Управляемые марковские процессы и их приложения. – М.: Наука, 1975. – 338 с.

REFERENCES

[1]. Future Aeronautical Communications / Edited by Simon Plass. – Institute of Communications and Navigation, German Aerospace Center (DLR), Germany. – Published by InTech Janeza Trdine 9, 51000 Rijeka, Croatia. – InTech, 2011. – 378 PP.

[2]. Tanenbaum, A.S. Computer Networks, 5th Ed. / Andrew S. Tanenbaum, David J. Wetherall. – Prentice Hall, Cloth, 2011, 960 PP.

[3]. Vodopianov S. Optimisation of Network Structures of Air Traffic Control Systems / Proceedings of the 6th International Conference "Advanced Computer Systems and Networks: Design an Application" ACSN-2013, Sept. 16-18, 2013, Lviv, Ukraine., P. 84-85.

[4]. Airlines Electronic Engineering Committee (AEEC). ARINC Report 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework, December 2005.

[5]. Mohd. Junedul Haque. An Approach for Intrusion Detection using HoneyPots to Improve Network Security // International Journal for Research in Applied Science & Engineering Technology (IJRASET)., Volume 3 Issue IV, April 2015, pp. 1029-1033.

[6]. Lenny Zeltser. Experimenting with Honeypots Using The Modern Honey Network 20 Feb 2015. – Electron Resource. Access mode: https://zeltser. com/modern-honey-network-experiments/

[7]. Tikhonov V.I., Mironov M.A. Markovian processes. Moscow.: Soviet Radio, 1977, 488 pp.

[8]. Druzhinin V.V., Kontorov D.C., Kontorov M.D. Introduction to conflict theory., M.: Radio and telecommunication, 1989., 288 pp.

[9]. Vinogradov N. A., Danilina G. V., Domarev D. V., Milokum Ja. V. Control pseudo-services in protected information systems on the basis of conflict theory //Scientific notes of Ukrainian scientific and research institute of telecommunication., 2014., №6(34), pp. 5-12.

[10]. Dynkin E.B., Jyshkevich A.A. Controlled Markovian processes and applications. – Moscow.: Science, 1975. – 338 pp.

ЗАХИСТ АВІАЦІЙНИХ БОРТОВИХ МЕРЕЖ ВІД АТАК МЕТОДАМИ ТЕОРІЇ КОНФЛІКТУ З ВИКОРИСТАННЯМ МЕДОВИХ ПАСТОК

Проблема захисту авіаційних бортових мереж від несанкціонованих вторгнень стоїть особливо гостро у зв'язку з необхідністю безумовного забезпечення безпеки польотів, усунення льотних подій і передумов до них. Для захисту мережі від зовнішніх і внутрішніх атак необхідно не просто підвищувати енергетичні і інформаційні ресурси, а застосовувати оптимальні методи боротьби з розумним супротивником. У ро-

боті запропоновані математичні моделі конфліктної взаємодії із застосуванням "медових пасток" – псевдо сервісів, що затягують супротивника в ескалацію атаки, що вимушує його витрачати свої енергетичні і інформаційні ресурси. Розроблена концептуальна модель побудови комбінованої системи захисту з упровадженим додатковим рівнем захисту – мережної медової пастки. Проведене комп'ютерне моделювання, результати якого свідчать про високу ефективність розробленого методу захисту мережі.
Ключові слова: авіаційна бортова мережа, теорія конфлікту, медова пастка, марківський процес, альтернуючий процес відновлення.

THE PROTECTION OF AVIATION BOARD NETWORKS FROM ATTACKS BY CONFLICT THEORY METHODS WITH HONEY POTS

The problem of protection of airborne networks from unauthorized encroachments stands especially sharply in connection with the necessity of the absolute providing of safety of flights, exception of flying incidents and preconditions to them. For protection of network from the external and internal attacks it is necessary not simply to raises power and informative resources, but apply the optimum methods of fight against a thinking opponent. The mathematical models of conflict co-operation with the use of "honey pots" – pseudo services tightening an opponent in escalation of attack are offered in work, forcing it to expend the power and informative resources. The conceptual model of construction of the combined system of protection with the inculcated additional level of protection – network honey pot is developed. The computer design is conducted, the results of which testify to high efficiency of the developed method of protection of network.
Keywords: airborne network, theory of conflict, honeypot, Markovian process, alternating process of renewal.

Водопьянов Сергей Вячеславович, соискатель, кафедра компьютерных систем и сетей Учебно-научного института Компьютерных информационных технологий Национального авиационного университета.
E-mail: s.vodopianov@abris-print.com.
Водоп'янов Сергій Вячеславович, здобувач, кафедра комп'ютерних систем та мереж Навчально-наукового інституту Комп'ютерних інформаційних технологій Національного авіаційного університету.
Vodopianov Sergey, applicant, of the computer systems and network department of educational and research institute of computer information technologies of National Aviation University (Kyiv, Ukraine).

Дрововозов Владимир Иванович, доцент кафедры компьютерных систем и сетей Учебно-научного института Компьютерных информационных технологий Национального авиационного университета.
E-mail: drovvlad@ukr.net.
Дрововозов Володимир Иванович, доцент кафедри комп'ютерних систем та мереж Навчально-наукового інституту Комп'ютерних інформаційних технологій Національного авіаційного університету.
Drovovozov Vladimir, associate professor of the computer systems and network department of educational and research institute of computer information technologies of National Aviation University (Kyiv, Ukraine).

Толстикова Елена Владимировна, доцент кафедры прикладной информатики Учебно-научного института Компьютерных информационных технологий Национального авиационного университета.
E-mail: tolstikova_alena@mail.ru.
Толстікова Олена Володимирівна, доцент кафедри прикладної інформатики Навчально-наукового інституту Комп'ютерних інформаційних технологій Національного авіаційного університету.
Tolstikova Elena, associate professor of the applied informatics department of educational and research institute of computer information technologies of National Aviation University (Kyiv, Ukraine).