информационно-деловой
ВЕСТНИК
ПАО ЦНПО «КАСКАД»
Качество - достойное Державы!

www.kaskad.ru vestnik@kaskad.ru Издается с 2005 года июль 2015 № 7 (124)

Здесь создается оружие будущего

ОБЪЕКТ

Противолодочные корабли получат новейшие крылатые ракеты

НОВОСТИ

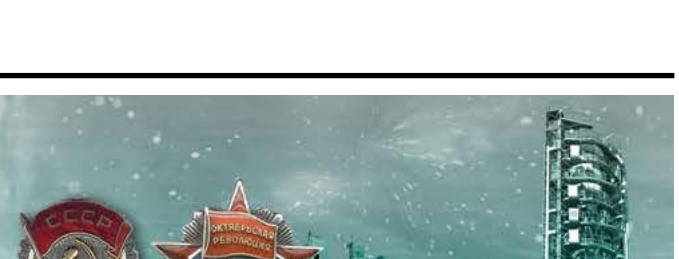
«Кинжал» для вражеского авианосца

НОВОСТИ

Может ли быть защита со 100%-ной гарантией? Обзор систем обнаружения вторжений

РЫНОК

ТЕМА НОМЕРА: Наш труд для российского флота



ОБЪЕКТ

Здесь создается оружие будущего

Дорогой стартов и побед
Наш полигон прошел немало.
В огне рождалась мощь ракет,
Рождалась в грохоте металла.

Мы покоряли рубежи
И шли вперед к ракетам новым.
Надежный курс нам проложил
Бессмертный гений Королева.

«Марш испытателей» Государственного центрального морского полигона

Государственный центральный морской ордена Ленина полигон МО РФ существует более 60 лет. Он старше Байконура. Датой основания считается 26 января 1954 года, когда Советом Министров СССР было принято постановление «О проведении проектно-экспериментальных работ по вооружению подводных лодок баллистическими ракетами дальнего действия и разработке на базе этих работ технического проекта большой ПЛ с реактивным вооружением». Лишь спустя год, когда практические работы по созданию полигона были уже в самом разгаре, ЦК КПСС и Совет Министров СССР совместным постановлением № 292-181сс утвердили создание Научно-исследовательского испытательного полигона № 5 Министерства Обороны СССР (НИИП № 5 МО СССР), предназначенного для испытаний ракетной техники (Байконур).

Тогда о полетах в космос речи еще не шло — нужно было возводить ракетный щит страны. И эта задача решалась именно здесь, на Двинской губе Белого моря, неподалеку от Северодвинска.

Капитан 1-го ранга В. И. Босый, начальник Государственного центрального морского ордена Ленина полигона МО РФ

Так был дан отсчет новой эре морского флота — эре ракетного оружия. Фактически ракетный полигон ВМФ СССР уже существовал в Феодосии на базе ракетного центра, однако для увеличения масштабов задач Белое море подходило куда лучше.

К весне 1955 года в городке Молотовск (как тогда назывался Северодвинск) была создана необходимая инфраструктура для первых испытаний. К созданию морской баллистической ракеты приступило КБ Королева, а Сергей Павлович стал главным конструктором первого ракетного комплекса для подводной лодки. К тому времени уже имелся определенный опыт создания ракетных комплексов наземного базирования (РІ, Р5, Р5М и Р11). Основу морского комплекса Д-1 составила баллистическая ракета Р-11ФМ на базе одноступенчатой оперативно-тактической ракеты наземного базирования Р-11. Ее ведущим конструктором Королев назначил молодого инженера И. В. Попкова. Новая ракета отличалась от своего прообраза другим горючим, окислителем, что отражалось на тактико-технических характеристиках (например, она имела меньшую дальность стрельбы). Однако для задач, которые ей предстояло решать, это принципиального значения не имело.

Затем 14 августа под командованием капитана третьего ранга Л. Ф. Алимова из Кронштадта на полигон прибыл корабль «Аэронавт» — плавучая лаборатория, оснащенная соответствующей измерительной техникой. Этот корабль сыграл значительную роль в испытаниях ракетного оружия для отечественного ВМФ.

В качестве носителя оружия ВМФ назначил ПЛ Б-67 проекта 611, которая прошла переоборудование на судостроительном заводе № 402 (Молотовск) под руководством И. С. Бахтина. Две ракетные шахты прорезали в диаметральной плоскости прочного корпуса ПЛ позади боевой рубки, охватив общим с нею ограждением. Итак, 14 сентября 1955 года ракету Р-11ФМ автотранспортом доставили с технической позиции в порт и с помощью крана «Аэронавта» начали погрузку на ПЛ Б-67. Первая в истории ВМФ погрузка ракеты на ПЛ завершилась на следующие сутки — утром 15 сентября в 4 часа 30 минут. 16 сентября 1955 года в 17 часов 32 минуты состоялся первый экспериментальный пуск ракеты Р-11ФМ с ПЛ Б-67 из надводного положения по боевому полю «Поной».

Во время пуска на ПЛ находился С. П. Королев. Так что

Продолжение на стр. 2

НОВОСТИ

Противолодочные корабли получат новейшие крылатые ракеты

БПК проекта 1155; по классификации НАТО — Udaloy (по названию первого корабля в проекте)

В преддверии профессионального праздника командование Военно-Морского Флота России сообщило журналистам информацию о том, что модернизированные большие противолодочные корабли (БПК) проекта 1155 (типа БПК «Удалой») будут вооружены крылатыми ракетами «Калибр» и «Оникс».

«ВМФ планирует модернизировать все восемь кораблей этого проекта, после модернизации срок их службы продлится еще на 10–15 лет», — заявил на проходившем недавно Военно-морском салоне главком ВМФ РФ адмирал Виктор Чирков. В составе ВМФ России находятся восемь кораблей этого проекта: четыре на Тихоокеанском флоте и четыре на Северном. «Первый корабль мы модернизируем через два года. Все эти корабли будут вооружены новыми ракетными комплексами “Калибр” и “Оникс”», — сказал главком. Сейчас это основные российские корабли дальней морской зоны — именно их отправляют в Аденский залив на борьбу с сомалийскими пиратами, которую Россия активно ведет с 2008 года.

Проект 1155 не нов. Кораблям исполнилось 30 лет, однако оснащение современными пушками А-192 «Армат», ракетами «Калибр» и новейшим комплексом ПВО и ПРО с ракетами от С-400 «Редут» серьезно увеличит их возможности. Благодаря такой переделке БПК

Продолжение на стр. 2

ОБЪЕКТ

Здесь создается оружие будущего

Начало на стр. 1

Из статьи Р. А. Журавлева «Состояние и перспективы развития полигонно-измерительного комплекса ГЦМП МО РФ» («Вестник ЮУрГУ» № 3 за 2012 год)

Большим шагом вперед является создание на базе полигона интегрированной автоматизированной системы (НАС) «Палтус», которая структурно является системой территориальной распределенной вычислительной сети сбора, совместной обработки и анализа радиотелеметрической и траекторной информации. Основная задача автоматизированной информационной системы «Палтус» заключается в том, чтобы снизить трудоемкость и повысить экономическую эффективность проводимых на полигонах испытаний и обеспечить достоверность оценки тактико-технических характеристик испытываемых образцов.

Автоматизированная информационная система имеет сложную структуру, в состав которой входят десятки компьютеров, серверы, коммуникационное и сетевое оборудование, периферийные устройства. Самый ближний пункт находится от центра сбора и обработки информации (ЦСОИ) на расстоянии 1 км, а самый отдаленный — 1000 км. С удаленных пунктов измерительная информация по наземным и спутниковым каналам связи поступает в ЦСОИ, где она по определенным правилам интегрируется, фильтруется, преобразовывается и подвергается специалистами анализу. Полученные результаты документируются на физических носителях. Источники информации для системы могут быть любыми. Заложенные оригинальные технические решения при проектировании системы при использовании низкоскоростных, широкополосных, проводных и спутниковых, аналоговых и цифровых каналов связи, развитая архитектура вычислительной сети, широкое использование современного коммуникационного оборудования, применение адаптеров и программно-математического обеспечения российского производства позволяют придать автоматизированной системе свойства относительной независимости и гибкости. При изменении типов источников информации базовая структура системы остается неизменной в зависимости от решаемых задач, при которых удаляются или добавляются отдельные компоненты системы и заменяется алгоритм обработки информации в ЦСОИ.

Внедренная на полигоне ИАС «ПАЛТУС» позволяет автоматизировать мероприятия ПИК, проводимые в ходе подготовки и проведения летных испытаний, и значительно повысить оперативность, качество, достоверность управления на всех этапах.

Технические и программные средства ИАС позволяют регистрировать, передавать по существующим каналам связи в реальном режиме времени, оперативно получать результаты испытаний, производить автоматизированную обработку измерений любых радиотелеметрических и внешнетраекторных систем, что способствует проведению качественных летних испытаний комплексов ракетного вооружения ВМФ.

Пуск ПКР П-800 «Оникс»

упоминание легендарного советского конструктора в тексте песни закономерно. Он действительно стоял у истоков полигона — это не просто красивая речевая фигура.

Испытательный пуск КР 3М-14 «Калибр» с ПЛА К-329

Итогом коллективного труда личного состава полигона и инженеров ОПК явилось принятие на вооружение первого морского комплекса Д-1 с ракетой Р-11ФМ. Таким образом, Советский Союз стал единственной страной в мире, в состав подводных сил которой вошли подводные лодки с баллистическими ракетами.

ЦНПО «КАСКАД» сотрудничает с ГЦМП МО РФ не первый год. В широкой кооперации с другими предприятиями ОПК Объединение участвовало в создании инфраструктуры полигона. В период с 2003 по 2005 год на полигоне совместно с представителями ОАО «КАСКАД» была развернута интегрированная автоматизированная система сбора, обработки и анализа телеметрической и траекторной информации по теме «Палтус». В октябре 2005 года данная система успешно прошла государственные испытания.

Об этой опытно-конструкторской разработке (ОКР) «КАСКАДА» стоит сказать особо. Фактически ее появление означало возвращение Объединения на прежние позиции в отрасли. По военно-морской тематике конец 1990-х был не самым стабильным временем для всего российского ОПК, и «КАСКАД» не стал исключением. Тем не менее работы по перспективным направлениям не прекращались ни на один день. Испытания разработки проходили в сложных условиях, так как ОКР по созданию опытного образца автоматизированной системы проводилась в очень сжатые сроки. Одновременно с созданием ИАС специалистами «КАСКАДА» велось восстановление телеметрических, радиолокационных и других систем полигона. Автоматизированная информационная система, разработанная специалистами ОАО ЦНПО «КАСКАД», имеет довольно сложную структуру (в ее состав входят десятки компьютеров, серверы, коммуникационное и сетевое оборудование, периферийные устройства, каналы и линии связи). Автоматизируемые объекты территориально удалены на тысячи километров. Эти особенности вызывали определенные сложности с обменом информацией между объектами заказчика. Трудности были связаны и с ограниченностью подготовленных специалистов узкой направленности. О масштабности проекта говорит

Пуск ракеты 3М-54 ракетного комплекса «Калибр-НК»

тот факт, что в работу по созданию системы и проведению испытаний были вовлечены специалисты центрального офиса, Белгородского, Ярославского, Знаменского филиалов, не считая полутора десятков контрагентов. Большую подготовительную работу проделала бригада монтажников Ярославского филиала.

Перед государственными испытаниями опытный образец информационной системы был подвергнут предварительным испытаниям. В их ходе проводились автономные проверки, затем — проверки подсистем, а в конечном итоге — проверка системы в целом. Интегрированная автоматизированная система была продемонстрирована представителям

Завершение на стр. 3

НОВОСТИ

Противолодочные корабли получат новейшие крылатые ракеты

П-800 «Оникс» (экспортное наименование — «Яхонт»; по классификации МО США и НАТО — SS-N-26 Strobile (англ. «шишка хвойного дерева»)) — советская/российская универсальная противокорабельная ракета среднего радиуса действия, предназначенная для борьбы с надводными военно-морскими группировками и одиночными кораблями в условиях сильного огневого и радиоэлектронного противодействия. Кроме того, может применяться против наземных целей; в данном случае дальность поражения цели может быть увеличена в несколько раз по сравнению со штатными 300 км в противокорабельном варианте.

Разработка оперативно-тактического противокорабельного комплекса четвертого поколения начата в конце 70-х годов XX века в ЦКБМ МОМ. В отличие от предшествовавших отечественных ПКР, имевших относительно узкую «специализацию» по носителям, новый комплекс с самого начала задумывался как универсальный: его предполагалось размещать на подводных лодках, надводных кораблях и катерах, самолетах и береговых пусковых установках.

ОКР «Калибр» (ранее объединены с ОКР «Бирюза»; по классификации НАТО — SS-N-27 Sizzler (англ. «испепелитель»)) — российские перспективные крылатые ракеты, которые разработаны и производятся ОКБ «Новатор».

Начало на стр. 1

станут фактически эсминцами и смогут уничтожать не только подводные лодки, но и надводные корабли, самолеты, ракеты, а также наземные объекты. То есть станут универсальными боевыми кораблями, как утверждают эксперты. По их оценкам, модернизация БПК 1155, обойдется в 2 млрд рублей за каждый корабль, тогда как стоимость строительства нового эсминца сравнимого уровня начинается от 30 млрд рублей.

Новый эсминец дальней морской зоны, который сможет заменить «Удалых», появится не раньше 2020 года. А новых кораблей такого же водоизмещения, как у БПК 1155, пока даже нет в проекте. Из всех остальных современных кораблей такие функции, как у него, есть только у фрегатов проекта 22350. Но они почти в два раза меньше, поэтому менее автономны (не могут отплывать далеко от базы) и несут меньше вооружения.

Противокорабельная ракета П-800 «Оникс» (в экспортном исполнении «Яхонт»), разработка конца 70-х годов ЦКБ МОМ

Экспортный вариант крылатой ракеты «Калибр» 3М-54Э1 на Морском салоне (Санкт-Петербург, июль 2015 года). Точные ТТХ некоторых модификаций засекречены

ОБЪЕКТ

Здесь создается оружие будущего

Начало на стр. 2

полигона, которые убедились в ее работоспособности на «живой» информации. Это был этап теснейшего взаимодействия специалистов ЦНПО «КАСКАД» и специалистов полигона, которым в дальнейшем пришлось эксплуатировать ИАС. Предварительные испытания показали, что основные технические и конструктивные решения, заложенные в систему, оказались правильными, функциональные характеристики были подтверждены. В ходе подготовки к государственным испытаниям было разработано, подготовлено, проверено и согласовано большое количество документов. Счет шел на тысячи листов схем, планов, перечней и т. д.

По оценкам многих специалистов, разработанная ОАО ЦНПО «КАСКАД» интегрированная автоматизированная система, которая комплексно решает задачи повышения качества и эффективности оценки тактико-технических характеристик испытываемых образцов вооружения, а также сокращения сроков проведения их испытаний, по-своему уникальна и создана впервые, во всяком случае для ВМФ. В ходе работ над созданием системы были поставлены и решены серьезные научно-технические задачи. Участники этого проекта были награждены памятными знаками и медалями в честь юбилея Государственного центрального полигона МО РФ.

ПАО ЦНПО «КАСКАД» и сегодня продолжает вести работы по данному проекту. Они предполагают постоянное совершенствование системы в рамках авторского надзора и сервисного обслуживания. В текущем году ПАО ЦНПО «КАСКАД» продолжает тесное сотрудничество с ГЦМП МО РФ. В условиях усложняющихся задач, решаемых полигоном, ЦНПО «КАСКАД» в кооперации с другими предприятиями ОПК наращивает свой технический потенциал с целью соответствовать требованиям, предъявляемым со стороны потенциального заказчика.

Работы в интересах ВМФ продолжаются. «КАСКАД» по-прежнему готов выполнить любую поставленную заказчиком задачу, причем выполнить ее на высоком инженерном уровне, точно в срок и с неизменным каскадовским качеством.

Стрельба ракетой Х-35, СКР «Татарстан», пр. 11661

НОВОСТИ

Морская доктрина России: задачи на глубине океана должны быть интегрированы с возможностями в космосе

26 июля 2015 года, в День ВМФ, в России была принята новая Морская доктрина. В этот день ее текст был опубликован на информационном ресурсе Президента РФ.

В российской Морской доктрине рассматривается в едином комплексе вся морская деятельность, как мирная, так и военная, весь морской транспорт и морские объекты, включая Военно-Морской Флот и глубоководные силы и средства Министерства обороны Российской Федерации, силы и средства органов Федеральной службы безопасности, а также рыбопромысловый, научно-исследовательский и специализированные флоты, объекты и средства разведки и добычи топливно-энергетических и минеральных ресурсов и других полезных ископаемых, организации национального кораблестроения и судостроения, а также инфраструктуру, обеспечивающую их функционирование и развитие всей морской структуры.

К 1980-м годам в СССР был создан второй по тоннажу военный флот в мире. Был создан класс самых современных АПЛ, и отечественное кораблестроение решало задачу создания современных ударных авианосцев. Сегодня Военно-Морской Флот является основой морского потенциала РФ, одним из инструментов внешней политики государства. ВМФ обеспечивает защиту национальных интересов РФ и ее союзников в Мировом океане военными методами. Он поддерживает военно-политическую стабильность и предназначен для отражения возможной агрессии с морских и океанских направлений. ВМФ обеспечивает военно-морское присутствие РФ, демонстрирует флаг и военную силу в Мировом океане, участвует в борьбе с пиратством и в гуманитарных операциях. ВМФ должен быть готов к решению перечисленных задач.

Общая российская военно-морская стратегия сугубо оборонительная. В качестве одной из основных целей российской национальной морской политики определена защита территории Российской Федерации от агрессии с океанских и морских направлений. Для этого РФ необходимо обладать «достаточным военно-морским потенциалом» и эффективно его использовать.

В Морской доктрине 2015 года восемь раз упоминается «мобилизационная готовность» как необходимый аспект разносторонней морской деятельности. Мобилизационная готовность означает системность военно-морской подготовки экипажей невоенных судов, руководящего состава судоходных компаний и органов государственного управления и их готовность к работе в условиях военного времени. В мобилизационной готовности должен находиться морской транспорт, рыбопромысловый, научно-исследовательский, а также специализированные флоты и организации, обеспечивающие их работу.

Современный российский ВМФ нуждается в интеграции с космическими войсками или даже более того — должен иметь в своем составе космическую группировку. Современные системы разведки и наведения оружия, подводные и воздушные роботы, «умные» мины, радиоэлектронная и киберборьба — все это в условиях конфликта не оставляет никаких шансов крупным надводным кораблям противника. Освоение российским ВМФ космического и киберпространства, больших глубин, овладение потенциалом электромагнитного спектра сделало бы его непобедимым.

НОВОСТИ

«Кинжал» для вражеского авианосца

Военно-морской салон, прошедший в начале месяца в Санкт-Петербурге, в очередной раз продемонстрировал возможности российского ОПК. Большой интерес специалистов вызвали представленные образцы ракет, предназначенных для поражения надводных целей. Эксперты признают: по ряду позиций этому оружию нет равных в мире.

Авиационная тактическая противокорабельная управляемая ракета Х-35УЭ (по классификации НАТО — AS-20 Kayak), в свое время пришедшая на смену технически устаревшей ракете «Термит», — настоящий «кинжал» для кораблей противника. Стремительно пролетая над водной поверхностью со скоростью, близкой к звуковой, она способна ударить по борту или надстройке корабля полутора сотнями килограммов боевого заряда. Ракету можно запускать даже при волнении моря в 6 баллов, при этом летит она над волной на высоте всего 3 м. Пусковая огневая установка (ракетный комплекс или самолет) может находиться на удалении от цели до 260 км.

Пусковыми установками для Х-35 являются корабельный ракетный комплекс «Уран» и береговой ракетный комплекс «Бал», а также самолеты и вертолеты. Для запуска используется отделяемый твердотопливный ускоритель, задающий ракете первоначальную скорость, после чего включается турбореактивный двигатель. В авиационном варианте ускорителя у ракеты нет: первоначальное ускорение придается скоростью самого летательного аппарата.

Уникальность ракеты в том, что, летя к заданной цели на высоте 10–15 м, она на конечном участке полета резко снижается до 3–5 м, «цепляя» объект атаки своей активной радиолокационной головкой самонаведения. На такой высоте и на такой скорости перехватить ракету средствами ПВО практически невозможно. Максимальная дальность стрельбы ракеты, как уже говорилось, составляет 260 км. Кроме того, в систему наведения Х-35УЭ добавлена аппаратура спутниковой навигации, благодаря чему модернизированная головка самонаведения позволяет захватывать цели уже на дальности 50 км, а не 20 км, как раньше.

Самолеты, с которых запускается это оружие, представляют всю номенклатуру современных авиационных боевых машин российского ВМФ: Су-30МК, Су-35, МиГ-29К, МиГ-29КУБ, МиГ-35. По сути, ракета может использоваться практически с любого самолета-носителя, на котором может быть подвешен контейнер или имеется бортовая система целеуказания с дальностью действия более 50 км. Есть планы включить модификацию Х-35 (Х-31АД) и в номенклатуру вооружения вертолета корабельного базирования Ка-52К. Интересно, что поражение цели может быть двух видов — с проникновением боевой части ракеты внутрь корабля и с подрывом над ним. В обоих случаях кораблю наносятся фатальные повреждения. В случае удара по авианосцу (по полетной палубе) из строя выводится оборудование для взлета-посадки самолетов (паровые катапульты), что превращает эти корабли практически в обычные круизные лайнеры.

информационно-деловой
ВЕСТНИК *ПАО ЦНПО «КАСКАД»*

РЫНОК

Может ли быть защита со 100% -ной гарантией?
Обзор систем обнаружения вторжений

Сетевые и информационные технологии меняются настолько быстро, что статичные защитные механизмы, к которым относятся системы разграничения доступа, межсетевые экраны, системы аутентификации, во многих случаях не могут обеспечить эффективную защиту. Поэтому требуются динамические методы, позволяющие оперативно обнаруживать и предотвращать нарушения безопасности.

В свое время известный литературный персонаж шутил: «100%-ную гарантию дает только страховой полис!». Действительно, когда речь заходит о современных технологиях, в том числе и технологиях сетевых атак, кажется, что никакая защита не обладает абсолютной надежностью. Тем не менее комплексный подход и высокий профессионализм интеграторов способны дать весьма обнадеживающий результат.

Для предотвращения несанкционированного доступа через сеть Интернет используется широкий спектр различных программных и аппаратных средств — система обнаружения вторжений (СОВ). Соответствующий английский термин — Intrusion Detection System (IDS) — активно употребляется и отечественными разработчиками.

Системы обнаружения вторжений обеспечивают дополнительный уровень защиты компьютерных систем. IDS сетевого уровня имеют много достоинств, которые отсутствуют в системах обнаружения атак на системном уровне. В действительности многие покупатели используют систему обнаружения атак сетевого уровня из-за ее низкой стоимости и своевременного реагирования. При этом надо понимать, что высокий уровень безопасности достигается только применением комплексных решений, причем с учетом индивидуальных особенностей деятельности компании.

Эффективность системы обнаружения атак во многом зависит от применяемых методов анализа полученной информации. В первых таких системах, разработанных в начале 1980-х годов, использовались статистические методы обнаружения атак. Автором первой концепции IDS считается Джеймс Андерсон, теоретически разработавший и опубликовавший принципы защиты. Но уже в 1984 году нашелся скептик, Фред Коэн, заявивший о том, что каждое вторжение обнаружить невозможно и что ресурсы, необходимые для обнаружения вторжений, будут расти вместе со степенью использования компьютерных технологий.

В настоящее время к статистическому анализу добавился ряд новых методик, начиная с экспертных систем и нечеткой логики и заканчивая использованием нейронных сетей.

Специфика статистического метода — использование уже разработанного и зарекомендовавшего себя аппарата математической статистики и адаптация к поведению субъекта. Сначала для всех субъектов анализируемой системы определяются профили. Затем любое отклонение используемого профиля от эталонного считается несанкционированной деятельностью. Статистические методы универсальны, поскольку для проведения анализа не требуется знания о возможных атаках и используемых ими уязвимостях. Однако статистические системы нечувствительны к порядку следования событий: в некоторых случаях одни и те же события в зависимости от порядка их следования могут характеризовать аномальную или нормальную деятельность; трудно задать граничные (пороговые) значения отслеживаемых IDS характеристик, чтобы адекватно идентифицировать аномальную деятельность. А главное — нарушители могут «ввести в заблуждение» статистические системы: их программы могут быть адаптированы таким образом, чтобы атакующие действия рассматривались как нормальные. Нужно также учитывать, что статистические методы неприменимы в случаях, когда для пользователя отсутствует шаблон типичного поведения или когда для пользователя типичны несанкционированные действия.

Более «продвинутыми» можно считать экспертные системы. Они состоят из набора правил, которые охватывают знания человека-эксперта. Другими словами, использование таких систем представляет собой распространенный метод обнаружения атак, при котором информация об атаках формулируется в виде правил. Эти правила могут быть записаны, например, в виде последовательности действий или в виде сигнатуры. При выполнении любого из них принимается решение о наличии несанкционированной деятельности.

Заметим, что системы защиты уже на самом раннем этапе развития включали в себя не только статистические, но и экспертные возможности. В частности, одна из первых моделей, появившаяся в 1986 году и сформировавшая основу для большинства современных систем, называлась IDES (Intrusion Detection Expert System — экспертная система обнаружения вторжений). Она функционировала на рабочих станциях Sun и проверяла как сетевой трафик, так и данные пользовательских приложений. IDES использовала два подхода к обнаружению вторжений: экспертную систему для определения известных видов вторжений и компонент обнаружения, основанный на статистических методах и профилях пользователей и систем охраняемой сети.

Вслед за IDES в 1993 году вышла NIDES (Next-generation Intrusion Detection Expert System — экспертная система обнаружения вторжений нового поколения). Незадолго до этого было реализовано обнаружение аномалий с использованием индуктивного обучения на основе последовательных паттернов пользователя на языке Common LISP. Программа была разработана для VAX 3500. Примерно в то же время был разработан NSM (Network Security Monitor — монитор сетевой безопасности), сравнивающий матрицы доступа для обнаружения аномалий на рабочих станциях Sun-3/50.

Важное достоинство такого подхода — практически полное отсутствие ложных тревог. База данных (БД) такой системы должна содержать сценарии большинства известных на сегодняшний день атак. Чтобы оставаться неизменно актуальными, экспертные системы требуют постоянного обновления БД. Хотя экспертные системы предлагают хорошую возможность для просмотра данных в журналах регистрации, требуемые обновления могут либо игнорироваться, либо выполняться администратором вручную. Как минимум это ослабляет возможности экспертной системы. В худшем случае отсутствие надлежащего сопровождения снижает степень защищенности всей сети, к тому же вводя ее пользователей в заблуждение относительно действительного уровня защищенности. Основным недостатком является невозможность отражения неизвестных атак. При этом даже небольшое изменение уже известной атаки может стать серьезным препятствием для функционирования системы обнаружения атак.

Большинство современных методов обнаружения атак используют некоторую форму анализа контролируемого пространства на основе правил или статистического подхода. В качестве контролируемого пространства могут выступать журналы регистрации или сетевой трафик. Анализ опирается на набор заранее определенных правил, которые создаются администратором или самой системой обнаружения атак.

Использование нейронных сетей является одним из способов преодоления указанных проблем экспертных систем. В отличие от экспертных систем, которые могут дать пользователю определенный ответ о соответствии рассматриваемых характеристик заложенным в БД правилам, нейронная сеть анализирует информацию и предоставляет возможность оценить, согласуются ли данные с характеристиками, которые она научена распознавать. В то время как степень соответствия нейросетевого представления может достигать 100 %, достоверность выбора полностью зависит от качества системы в анализе примеров поставленной задачи. Важным преимуществом нейронных сетей при обнаружении злоупотреблений становится их способность «изучать» характеристики умышленных атак и идентифицировать элементы, которые не похожи на те, что наблюдались в сети прежде.

Различные методы защиты основаны на разных принципах действия. Хотя и СОВ, и межсетевой экран относятся к средствам обеспечения информационной безопасности, последний отличается тем, что ограничивает поступление на хост или подсеть определенных видов трафика для предотвращения вторжений и не отслеживает вторжения, происходящие внутри сети. СОВ, напротив, пропускает трафик, анализируя его и сигнализируя при обнаружении подозрительной активности. Обнаружение нарушения безопасности проводится обычно с использованием эвристических правил и анализа сигнатур известных компьютерных атак.

Сейчас трудно встретить систему, реализующую только один из описанных методов. Как правило, они используются в совокупности.

Главный редактор М. Сарбучев
Корректор Ю. Соболевская
Верстка О. Добренкова

Россия, 125047, Москва,
1-я Брестская ул., 35
Телефон: (499) 978-58-73,
(495) 251-76-50
Факс: (499) 978-57-36
E-mail: vestnik@kaskad.ru
http://www.kaskad.ru

Тираж 999 экз.

Распространяется по уникальной базе ОАО ЦНПО «КАСКАД»