УДК 004.413.2

РАЗРАБОТКА НАУЧНЫХ МЕТОДОВ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ

Черненко С.С.[1], Назаренко М.А.[1]

[1]*ФГБОУ ВПО «Московский государственный технический университет радиотехники, электроники и автоматики», mirea.dubna@mail.ru.*

В статье рассмотрена проблема разработки методов обеспечения безопасности компьютерных сетей с точки зрения научной методологии. Выявлены методологические аспекты, связанные с современным уровнем развития компьютерных технологий, а также с тенденциями развития таковых в применении к сетевым коммуникациям. Обоснована необходимость парадигмального перехода концепции защиты сетей с метода «укреплённой крепости» на динамическую защитную систему, обеспечивающую постоянный мониторинг процессов и оперативное реагирование на нежелательные события, а также дальнейший учёт актуального опыта, что позволит модифицировать тактические алгоритмы противодействия нарушениям защиты. Указано на необходимость использования междисциплинарного подхода, в частности — применение опыта построения схем моделирования надежности сложных технических систем из последовательно-параллельных соединений элементов, для каждого из которых известны количественные характеристики параметров надежности.

Ключевые слова: компьютерные сети, защита информации, политика безопасности.

DEVELOPMENT OF SCIENTIFIC METHODS OF COMPUTER NETWORK DEFENSE

Chernenko S.S.[1], Nazarenko M.A.[2]

[1]*Dubna branch of Moscow State Technical University of Radioengineering, Electronics and Automation, mirea.dubna@mail.ru.*

The article considers the problem of developing methods to ensure the defense of computer networks from the point of view of scientific methodology . The methodological aspects of the current state of computer technology and development trends such as applied to network communications . Necessity of paradigmatic transition from concept to protect networks method "fortresses" in a dynamic defense system that provides continuous monitoring of processes and rapid response to adverse events, as well as further consideration of actual experience, which will modify the algorithms tactical counter to defense breaches. The necessity of an interdisciplinary approach , in particular - the use of experience diagramming reliability modeling of complex technical systems of series-parallel connections of elements, each of which are known quantitative characteristics of reliability parameters .

Keywords: computer networks, information security, security policy.

Ускорение информационных процессов в современном мире приводит к возрастающей роли информационной среды. Действия над материальными объектами всегда сопровождаются действиями над соответствующей информацией, а в ряде сфер работа осуществляется исключительно над нематериальными информационными объектами.

Вследствие распространённости информационных компьютерных сетей вопрос их безопасности становится всё более актуальным. Основной проблемой защиты компьютерных сетей является виртуальность деятельности соответствующего направления, а также многофакторность уязвимостей — от аппаратного обеспечения до человеческого фактора.

Усугубляет ситуацию психологическое восприятие нематериальных объектов, в частности информации, как маловажной, по мнению значимого количества неспециалистов. Таким образом, если нанесение материального ущерба или осуществление акта хищения материальной собственности считает возможным незначительное количество людей, то

нанесение ущерба программному обеспечению, хранимой информации и т.д. для большинства психологически осуществляется гораздо легче. При этом речь идёт не только о злоумышленниках, но и о небрежном и некомпетентном отношении к работе с информацией и др.

В настоящее время имеется значительное число публикаций по различным аспектам безопасности компьютерных сетей, а именно:

- контроль доступа;
- криптография данных;
- отказоустойчивость;
- надёжность хранения информации;
- защищённость сетевых протоколов;
- борьба с сетевыми атаками;
  - физические аспекты безопасности;
  - сохранение непрерывности бизнес-процессов
- и другие.

Вышеперечисленные и иные аспекты обеспечения безопасности компьютерных сетей практически всегда рассматриваются независимо друг от друга, без разработки общего подхода к проблеме безопасности. При этом, как правило, анализ конкретного аспекта подаётся с профессиональной точки зрения узкого специалиста, что в конечном итоге не отражает проблемы в целом. Специфические виды угроз должны анализироваться и предотвращаться специалистами, но при этом необходима интеграция методов защиты в единую многоаспектную систему, а также разработка общеметодологического подхода к теме безопасности компьютерной сети как системы, имеющей связь с внешней средой.

Классическая схема защиты информации по принципу «периметра безопасности» не соответствует современности. Требуется разработка концепции, адекватной текущим технологическим возможностям, и основанной на постоянном мониторинге ситуации, готовности оперативно реагировать на нежелательные события в системе и дальнейшем учете актуального опыта, позволяющем модифицировать тактические алгоритмы противодействия нарушениям защиты.

Современный стандарт управления информационной безопасностью компьютерных сетей предприятия должен содержать систему методов, направленную на достижение состояния постоянной готовности сети к возникающим непредвиденным обстоятельствам.

Одна из самых распространённых ошибок в построении системы защиты компьютерных сетей — это замена создания действенной защиты получением сертификата, подмена научного подхода бюрократическим. Такой метод очень удобен для отчётности, чем

и обуславливается его популярность. Наглядно недопустимость сведения политики безопасности к простому следованию сертификатов показана в книге Дж. Седдона «В поисках качества. Дело против ISO 9000», в которой он указывает на то, что получение сертификата создаёт иллюзию решения проблем, в том числе — и в области управления информационной безопасностью. Стандарты ISO 9000 делают отчёты способом управления деятельностью компании, продвигают концепцию обеспечения качества методом проверок, а не постоянного контроля производственных и бизнес-процессов, препятствуют разработке собственных взглядов на проблему.

Таким образом, с современной научной точки зрения в модели обеспечения безопасности компьютерных сетей защита активов является не единственной задачей системы, а лишь одним из элементов системы управления безопасностью. Если ранее, при использовании парадигмы «защищённой крепости», ставилась задача обеспечения заданного уровня безопасности при минимизации затрат, то на современном уровне защита активов является лишь одним из критериев качества системы защиты [7].

Для компьютерных специалистов важно понимать не только программную или только аппаратную часть комплекса согласно своей узкой специализации, но и иметь представление об остальных подсистемах сети. Примером грамотного подхода может служить обучение в филиале МГТУ в г. Дубна, где студенты, обучающиеся по специальности «Вычислительные машины, комплексы, системы и сети», изучают терминальные системы, что позволяет понимать вопросы монтажно-наладочной, а также сервисно-эксплуатационной деятельности [11] — в том числе и с точки зрения обеспечения безопасности работы терминального узла, что оказывает влияние на отказоустойчивость компьютерной сети в целом.

Особое внимание следует уделять серверному оборудованию — вследствие этого оно должно обслуживаться квалифицированными специалистами. Персональные компьютеры сотрудников должны рассматриваться как узлы с повышенной степенью риска. Несмотря на то, что обычно уровень доступа обычного пользователя не позволяет выйти на уровень работы с серверами в целом, возможность нарушения работы в своём сегменте остаётся значимым фактором. При этом персональный компьютер может быть использован для получения доступа к данным работающего с ним специалиста, а также вероятно использование его как узла для получения доступа к другим частям сети. С каждым годом этот аспект безопасности требует всё большего внимания в связи с распространением на рабочих местах ноутбуков вместо стационарных рабочих компьютеров. Роль кадрового аудита в современных организациях значительна [5], но вопросу компьютерной грамотности и ответственности в плане информационной безопасности уделяется явно недостаточное внимание. Целесообразно не просто запрашивать уровень компьютерных навыков

пользователя при приёме на работу, но и проводить проверку соответствующих компетенций, создавать соответствующую организационную культуру в компании на основе социального партнёрства, вовлечения сотрудников в понимание важности проблемы [6], что важно для успешного функционирования организации в целом [12].

В плане безопасности сетей стандартный метод разграничения уровня доступа также не отвечает требованиям современности, поскольку задаются рамки: во-первых, слишком жёсткие, во-вторых, статические. Таким методом можно ограничить права до минимальных, но если сотрудник в процессе работы использует многочисленные базы данных из разных областей, то зачастую он получает полноценный постоянный доступ к информации, между тем как ему необходим лишь периодический. Д.А. Подкорытов разработал современную модель политики безопасности вычислительных систем, которую образно описывает следующим образом [15]:

«В традиционной политике предоставления доступа правила доступа формулируются исходя из статического состояния системы: “Через эту дверь аутентифицированный субъект проходить может”. По мнению автора, необходимо учитывать и динамику: “Через эту дверь проходить можно, но не более одного раза в секунду для каждого субъекта, при условии, что информационная система находится в некотором состоянии Б”».

Описанный динамический системный контроль уровня доступа, согласно происходящим в системе процессам, требует постоянной поддержки контакта заказчика программного обеспечения с исполнителем работ для своевременной модернизации системы контроля, что соответствует принципам современного подхода к менеджменту качества [10], которые подразумевают постоянное улучшение соответствующих систем контроля и управления [2], что должно являться одной из постоянных и основных целей организации [9].

В качестве примера информационной сети, которая имеет дифференциацию по логической структуре, можно привести компьютерную сеть образовательного учреждения, которую целесообразно разделить на информационные блоки: финансовый (бухгалтерский), административный и учебно-организационный с выделением особого блока приёмной комиссии [8], который должен находиться под особым контролем по фактам доступа. При этом мониторинг образовательных процессов должен обеспечиваться динамическим сбором учебных показателей, поскольку данные от дискретных контрольных мероприятий могут не только ненамеренно искажать фактическое положение дел [13], но и быть фальсифицированы с большей лёгкостью, что также означает уязвимость в плане информационной безопасности.

Концепция повышения безопасности компьютерных сетей посредством анализа сетевого трафика имеет хорошие перспективы. К её преимуществам относится скорость

реагирования на угрозы, а также отсутствие необходимости анализа содержимого проходящих пакетов. При этом метод может применяться как к внутренней, так и внешней сети, а методы обнаружения аномальной активности поддаются численному анализу [1], что позволяет создавать программные продукты, осуществляющие мониторинг безопасности в режиме реального времени [14].

При разработке подобных систем контроля следует учитывать, что каналы связи, в отличие от узлов компьютерной сети, нередко подвержены несанкционированному воздействию, не имеющему причиной человеческий фактор. Возможны нарушения линий связи вследствие естественных причин, природных факторов и др., поэтому для обеспечения непрерывности работы требуется наличие резервных каналов связи.

При разработке научных методов обеспечения защиты компьютерных сетей следует использовать междисциплинарный подход. Так, для создания моделей надежности сложных технических систем широко применяются схемы, состоящие из последовательно-параллельных соединений элементов, для каждого из которых известны количественные характеристики параметров надежности [3]. Однако такой подход редко применяется для систем защиты информации. Не смотря на то что проблема структуризации компьютерной сети с однозначным выделением элементов схемы может быть решена [4], необходимо учитывать не только аппаратные факторы, как в технике, но и программные и человеческие, которые моделируется как подсистемы общей системы сети.

Особо следует отметить тот факт, что в практической деятельности компаний ущерб от нарушения информационной безопасности не всегда рассматривается как таковой: зачастую предпринимаются попытки снижения риска иными методами — экономическими, юридическими и др. В большинстве случаев это гораздо менее эффективно, чем устранение причин риска в информационной сфере.

Стандартные методы защиты информации разрабатываются длительное время и подразделяются на:

а) аппаратные методы защиты, включая аппаратные шифровальные ключи и устройства идентификации характеристик человека (голос, отпечатки пальцев и сетчатки);

б) программные методы защиты, что включает идентификацию технических средств, задач и пользователей в сети, распределение прав, контроль их работы и др.;

в) резервное копирование данных, включая «горячее» при помощи RAID-массивов;

г) криптографическое шифрование информации;

д) физические меры защиты, включая изоляцию от посторонних помещений и сооружений, в которых установлена соответствующая аппаратура;

е) организационные мероприятия по защите информации, т.е. нормативно-правовые акты, регламентирующие деятельность компьютерной сети, а также работу персонала.

Угрозы безопасности компьютерной сети целесообразно разделять на внутренние (возникающие внутри компании) и внешние, а также на активные (имеющие целью нарушение функционирования сети) и пассивные (несанкционированное использование информационных ресурсов без нарушения функционирования сети). Наиболее частым случаем пассивной угрозы является несанкционированный доступ, то есть преднамеренное противоправное овладение информации лицом, не имеющим права доступа к таковой. На этом примере целесообразно пояснить разнообразие и сложность рисков, которые должны учитываться при разработке методик защиты компьютерных сетей:

- в области программного обеспечения возможно использование специально написанных вирусов и других вредоносных программных продуктов, использование «уязвимых мест» операционных систем и других программ, несанкционированный доступ в сеть через уязвимые протоколы передачи данных;
- в области материально-технического обеспечения возможно копирование носителей информации (в т.ч. с преодолением мер защиты), но в качестве высокотехнологических способов промышленного шпионажа для несанкционированного доступа к информации могут быть применены методы снятия электромагнитных колебаний с дальнейшей расшифровкой информации и др.;
- человеческий фактор, при этом может иметь место факт намеренного сотрудничества с конкурентном и др., а возможна небрежность вида предоставления доступа к работе под своей учётной записью, небрежное хранение паролей и т.д.

Разработка защиты компьютерных сетей с использованием научно-методологического подхода в первую очередь означает моделирование компьютерной сети как сложной системы, состоящей из подсистем, соответствующих технической аппаратуре, программному обеспечению и человеческому фактору, при этом имеющей каналы связи с внешним миром. Необходимо учитывать воздействие на потенциально уязвимые места такой системы со стороны как аппаратного, так и программного воздействия, а также последствия деятельности сотрудников, как злонамеренной, так и случайной вследствие некомпетентности либо безответственности. При этом необходим динамический мониторинг состояния сети с оперативным предотвращением возникающих угроз.

Список литературы

1. Ажмухамедов И.М., Марьенков А.Н. Обеспечение информационной безопасности компьютерных сетей на основе анализа сетевого трафика // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. — 2011. — № 1. — С. 137–141.
2. Акимова Т.И., Мельников Д.Г., Назаренко М.А. Применение принципа постоянного улучшения систем менеджмента качества в учебном процессе // Международный журнал прикладных и фундаментальных исследований. — 2014. — № 3. — С. 126–128.
3. Баранова А.В., Ямпурин Н.П. Основы надежности электронных средств. — М. : Академия, 2010. — 234 с.
4. Булгаков О.М., Удалов В.П., Кучмасов Е.А. Принципы построения модели надежности системы защиты информации // Вестник ВИ МВД России. — 2012. — № 3. — С. 167–176.
5. Горшкова Е.С., Назаренко М.А., Алябьева Т.А., Корешкова А.Б., Фетисова М.М. Роль кадрового аудита в организации // Международный журнал прикладных и фундаментальных исследований. — 2013. — № 10 (ч. 2). — С. 330-331.
6. Духнина Л.С., Лысенко Е.И., Назаренко М.А. Основные принципы социального партнерства в сфере труда и доверие к ним со стороны работающей молодежи // Международный журнал экспериментального образования. — 2013. — № 4. — С. 174–175.
7. Королева Н.А. Экспертная система поддержки принятия решений по обеспечению информационной безопасности организации : дис. … канд. тех. наук. — Тамбов, 2006. — 198 с.
8. Лысенко Е.И., Черненко С.С. Организация сети образовательного учреждения // Международный журнал прикладных и фундаментальных исследований. — 2014. — № 3. — С. 128–129.
9. Назаренко М.А. Межпредметные связи теории организаций, организационной культуры и кадрового аудита // Международный журнал прикладных и фундаментальных исследований. — 2013. — № 10 (ч. 3). — С. 518–519.
10. Назаренко М.А., Адаменко А.О., Киреева Н.В. Принципы менеджмента качества и системы доработки или внесения изменений во внедренное программное обеспечение // Успехи современного естествознания. — 2013. — № 7. — С. 177–178.
11. Назаренко М.А., Белолаптикова А.И., Лысенко Е.И. Вычислительные комплексы и системы — терминальные системы в рамках ФГОС ВПО // Успехи современного естествознания. — 2013. — № 6. — С. 158–159.
12. Назаренко М.А., Петров В.А., Сидорин В.В. Управление организационной культурой и этический кодекс вуза // Успехи современного естествознания. — 2013. — № 4. — С. 171–172.

13. Никонов Э.Г., Назаренко М.А. Модель кафедры в системе менеджмента качества // Международный журнал прикладных и фундаментальных исследований. — 2013. — № 1. — С. 146.
14. Ниссенбаум О.В., Присяжнюк А.С. Адаптивный алгоритм отслеживания аномальной активности в компьютерной сети на основании характерных изменений оценок альтернирующего потока // Прикладная дискретная математика (Приложение). — 2010. — № 3. — С. 55–58.
15. Подкорытов Д.А. Модель политики безопасности вычислительных систем // Информационно-управляющие системы. — 2004. — № 1. — С. 41–49.

Рецензенты:

Никонов Э.Г., д.ф.-м.н., старший научный сотрудник, заведующий кафедрой информационных технологий МГТУ МИРЭА (Министерство образования и науки Российской Федерации), г. Дубна.

Омельяненко М.Н., д.т.н., профессор, заведующий кафедрой промышленной электроники МГТУ МИРЭА (Министерство образования и науки Российской Федерации), г. Дубна.