**СОДЕРЖАНИЕ**

Введение

1. Технология анализа защищенности

2. Технология обнаружения воздействия нарушителя

3. Технология защиты информации от НСД

4. Технология антивирусной защиты

Заключение

Список литературы

# Введение

Под информационной безопасностью понимают защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. (Чуть дальше мы поясним, что следует понимать под поддерживающей инфраструктурой.)

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

1. Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае "пусть лучше все сломается, чем враг узнает хоть один секретный бит", во втором – "да нет у нас никаких секретов, лишь бы все работало".
2. Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте.

Возвращаясь к вопросам терминологии, отметим, что термин "компьютерная безопасность" (как эквивалент или заменитель ИБ) представляется нам слишком узким. Компьютеры – только одна из составляющих информационных систем, и хотя наше внимание будет сосредоточено в первую очередь на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее безопасность определяется всей совокупностью составляющих и, в первую очередь, самым слабым звеном, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой пароль на "горчичнике", прилепленном к монитору).

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Эта инфраструктура имеет самостоятельную ценность, но нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций.

Обратим внимание, что в определении ИБ перед существительным "ущерб" стоит прилагательное "неприемлемый". Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений.

Информационная безопасность телекоммуникационных систем является одним из важных аспектов информационной безопасности государства в целом. Можно выделить целый ряд очевидных факторов, существование которых придаст проблеме информационной безопасности телекоммуникационных систем особую актуальность при формировании системного взгляда на современную жизнь общества и государства.

Проблемы информационной безопасности государства в нынешних условиях являются неотъемлемой частью жизни современного общества. Более того, они стали важнейшими задачами внутренней и внешней политики многих государств мира. Активное обсуждение вопросов обеспечения информационной безопасности инфокоммуникационных систем России на проходящих научных и научно-технических конференциях, а также на страницах специальных изданий свидетельствует о большой актуальности многих ключевых проблем, связанных с появлением новых видов информационного оружия, серьезными разрушительными послед­ствиями его применения, недостаточной эффективностью возможных средств защиты и т.д. Не выработаны до сих пор и достаточно эффективные пути решения этих проблем.

# 1. Технология анализа защищенности

Технология анализа защищённости представляет собой совокупность методов обнаружения технологических и эксплуатационных уязвимостей ПО АС [11]. Данная технология реализуется при помощи систем анализа защищённости или сканеров безопасности, представляющих собой специализированное ПО. Рассмотрим более подробно методы выявления технологических и эксплуатационных уязвимостей и проанализируем возможность использования существующих средств, реализующих эти методы, для выявления уязвимостей ПО узлов ГСПД и ЦУС.

Существующие средства анализа защищённости, реализующие метод анализа исходных текстов ПО, не могут быть использованы для обнаружения технологических уязвимостей ПО узлов ГСПД и ЦУС, поскольку основная часть исходных текстов ПО узлов ГСПД и ЦУС является «закрытой», т. е. интеллектуальной собственностью производителей ПО, и не подлежит распространению вне рамок компании-разработчика. Процедура же дезассемблирования, которая может быть применена для получения исходного кода ПО узлов ГСПД и ЦУС из исполняемых модулей программ, не может однозначно гарантировать, что полученный в результате этой процедуры исходный код соответствует дизассемблированной программе. Это связано с тем, что в процессе дезассемблирования не всегда имеется возможность определить разницу между исполняемыми командами и данными программы.

Обнаружение технологических уязвимостей ПО АС при помощи анализа исполняемого кода ПО осуществляется путём запуска программы АС в рамках тестовой среды, которая проверяет правильность выполнения этой программы. В процессе выполнения программы для неё формируется ряд запросов, после чего анализируется реакция тестируемой программы, т.е. каким образом исполняемый код программы влияет на состояние тестовой среды. Если в результате сформированного запроса тестовая среда переходит в небезопасное состояние, приводящее, например, к нарушению работоспособности АС, то делается вывод о наличие ряда уязвимостей в тестируемой программе. Такой метод обнаружения уязвимостей позволяет выявить ряд ошибок, внесённых на технологическом этапе, например ошибки, приводящие к переполнению буфера, ошибки неправильного доступа к памяти, выход за границы массива данных и др. Основным недостатком рассмотренного метода является отсутствие гарантий обнаружения всех технологических уязвимостей ПО АС, поскольку смоделировать все возможные состояния среды, в рамках которой выполняется программа АС, не представляется возможным.

Существующие средства обнаружения технологических уязвимостей при помощи анализа исполняемого кода могут быть использованы только для анализа защищённости ПО ЦУС, поскольку оно базируется на стандартных ОС. В настоящее время на отечественном рынке ИБ отсутствуют средства анализа защищённости ПО узлов ГСПД, которые используют специализированные ОС. Последний способ обнаружения технологических уязвимостей заключается в имитации ВН на АС и анализе результатов моделирования этих ВН. В случае, если процесс моделирования ВН завершается успехом, то система делает вывод о наличии уязвимости в ПО тестируемой АС.

Рассмотренные выше средства анализа защищённости, функционирующие посредством имитации ВН, могут быть использованы для выявления уязвимостей ПО как узлов ГСПД, так и ЦУС. Тем не менее, необходимо отметить, что в настоящее время системы этого класса, представленные на отечественном рынке ИБ, могут применяться только в ГСПД, функционирующих на основе стека протоколов ТСР/IР.

Выявление эксплуатационных уязвимостей АС может осуществляться двумя способами: при помощи проверки настроек программно-аппаратного обеспечения АС или посредством имитации ВН на АС. Проверка настроек заключается в выявлении тех параметров работы программно-аппаратного обеспечения АС, которые могут быть использованы нарушителем при реализации воздействия. Процедура имитации ВН реализуется рассмотренными выше средствами моделирования атак, предназначенными для обнаружения технологических уязвимостей. Средства выявления эксплуатационных уязвимостей также могут быть использованы для анализа защищённости узлов ГСПД и ЦУС.

Проведённый анализ существующих на отечественном рынке средств выявления технологических и эксплуатационных уязвимостей показывает, что ни одно из существующих средств не позволяет гарантировать стопроцентное обнаружение всех уязвимостей, присутствующих в ПО узлов ГСПД и ЦУС. Так, например, в настоящее время отсутствует возможность обнаружения при помощи систем анализа защищённости тех «закладок», подробное описание параметров которых не заложено в систему анализа защищённости.

# 

# 2. Технология обнаружения воздействия нарушителя

Технология обнаружения ВН представляет собой совокупность методов обнаружения атак нарушителя на АС [14, 23]. Данная технология реализуется при помощи специализированных программно-аппаратных комплексов, называемых системами обнаружения ВН, выполняющими две основные функции:

- формирование банка данных, содержащего сведения о работе АС, который впоследствии может быть использован для выявления ВН на АС, защищаемые системой обнаружения ВН. Банк данных, формируемый системой обнаружения, может включать в себя: параметры заголовков сообщений, поступающих в АС, время, количество и объём данных, поступающих в АС, число установленных логических соединений с АС за единицу времени, текущий уровень загрузки АС, контрольные суммы программного обеспечения АС и др.;

- определение на базе сформированного банка данных фактов проведения ВЫ на информационные ресурсы и инфраструктуры АС, защищаемых системой обнаружения.

Первую функцию систем обнаружения ВН выполняют сенсоры, а вторую - анализаторы. Настройка параметров работы сенсоров и анализаторов осуществляется центром управления системой обнаружения ВН. В настоящее время существует два основных типа сенсоров: сенсоры, функционирующие на базе анализа журналов аудита АС, и сенсоры, функционирующие на базе анализа трафика, передаваемого по каналу связи, к которому подключена АС.

Основная задача сенсоров, функционирующих на базе анализа журналов аудита АС, заключается в формировании банка данных, содержащего сведения о работе АС. Такой банк данных создаётся на базе регистрационных записей журналов аудита, формируемых АС. Схематично структура системы обнаружения ВН, включающая сенсоры, функционирующие на базе анализа журнала аудита, изображена на рис. 1.

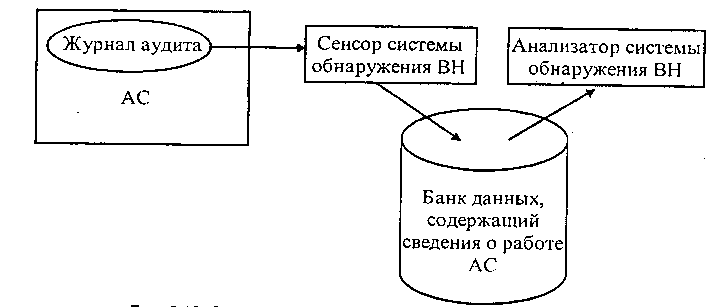


рис.1. Структура системы обнаружения ВН

Недостатком сенсоров, функционирующих на базе анализа журналов аудита АС, является платформенная зависимость, поскольку необходимая для системы обнаружения ВН информация по-разному представлена в различных ОС, под управлением которых функционируют АС. Так, например, характер представления регистрационной информации в журналах ОС рабочих станций пользователей отличается от варианта представления ОС, используемой в большинстве серверов.

К преимуществам сенсоров, функционирующих на базе анализа журналов аудита АС, можно отнести относительно небольшой объём и высокую точность данных, извлекаемых сенсором из журналов аудита АС. Поскольку извлечённая информация не требует дальнейших преобразований и готова к обработке, то системы обнаружения с сенсорами на базе анализа журнала аудита АС обладают высоким быстродействием.

Основная задача сенсоров, функционирующих на базе анализа трафика, заключается в перехвате сообщений, передаваемых по каналам связи, к которым подключена АС, и формировании банка данных, содержащего информацию о работе АС. Критерии перехвата сообщений должны задаваться администратором безопасности. Схематично структура системы обнаружения ВН с сенсорами на базе анализа сетевого трафика отражена на рис. 2.4.

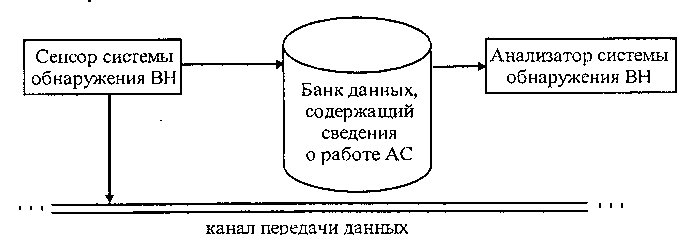


рис.2. Структура системы обнаружения

После того как сенсор осуществил перехват сообщения, он должен извлечь из заголовка сообщения и поместить в банк данных системы обнаружения необходимую информацию, такую как типы и параметры протоколов, используемых для формирования сообщений, поступающих в АС, время, количество и объём передаваемых сообщений и др. Накопленный в базе данных материал позволит анализатору системы сделать вывод о наличии ВН на АС.

В сравнении с сенсорами, функционирующими на базе анализа журналов аудита АС, данный тип сенсоров, базирующийся на анализе канального трафика, позволяет получать больший объём информации о работе АС, что позволяет обнаруживать большее число ВН. Так, например, сенсоры, функционирующие на базе анализа журналов аудита, как правило, не фиксируют аппаратные адреса АС, обменивающихся между собой сообщениями, что позволяет нарушителю выполнить несанкционированные действия путём фальсификации своего аппаратного адреса. В этом случае обнаружить ВН этого типа способна лишь система обнаружения, включающая сенсоры, функционирующие на базе анализа канального трафика. Другим преимуществом сенсоров этого типа является высокая степень отказоустойчивости. Это объясняется тем, что сенсоры, функционирующие на базе анализа журналов аудита, жёстко привязаны к АС, на которой хранится журнал, т.е. в случае выведения из строя АС перестанет функционировать и сенсор. В то же время сенсоры, функционирующие на основе анализа канального трафика, устанавливаются в каналы связи и не зависят от работоспособности окружающих их АС.

Деятельность организации обеспечивается системой взаимоувязанной управленческой документации. Её состав определяется компетенцией структурных подразделений организации, порядком разрешения вопросов (единоначальный или коллегиальный), объёмом и характером взаимосвязей между организацией и его структурными подразделениями, другими органами управления и организациями.

Процесс выявления и регламентации состава информации – это тайна фирмы, являющаяся основополагающей частью системы защиты информации. Состав этих сведений фиксируется в специальном перечне, где закрепляется факт отнесения их к защищаемой информации и определяющий период конфиденциальности сведений, уровень или гриф секретности, а также список лиц, которые имеют право использовать их сведения.

Ценность информации и требования к её надежности находятся в прямой зависимости. Ценность информации может быть выражена в денежном эквиваленте и характеризовать конкретный размер прибыли при её использовании или размер убытков при её потере. Производственная или коммерческая ценность недолговечна и определяется временем, необходимым конкурентам для выработки той же идеи или её хищения.

# 3. Технология защиты информации от НСД

Технология защиты информации от НСД [9] представляет собой совокупность методов и средств защиты информационных ресурсов и инфраструктур АС от несанкционированного ознакомления и обработки, включая защиту от несанкционированной модификации, уничтожения или копирования информации. Технология защиты информации от НСД базируется на проведении процедуры идентификации и аутентификации субъектов доступа к этой информации. В качестве аутентификационных параметров доступа могут выступать:

- пароли, вводимые пользователем с клавиатуры;

- смарт-карты;

- идентификаторы;

- электронные 118В-ключи;

- криптографические ключи пользователя;

- биометрические параметры пользователя и др.

Обобщённый алгоритм работы средств, построенных на базе технологии защиты информации от НСД, выглядит следующим образом. На этапе получения доступа к какому-либо информационному ресурсу или инфраструктуре АС средства защиты запрашивают аутентификационные параметры субъекта доступа и сравнивают их со значениями, хранящимися в БД средства защиты. В случае установления соответствия между сравниваемыми величинами субъекту разрешается доступ к соответствующим ресурсам и инфраструктурам АС. В противном случае средство защиты информации от НСД несколько раз повторяет запрос на повторный ввод аутентификационных данных, после чего блокирует доступ к АС и сигнализирует администратору безопасности о попытке получения НСД. В случае если АС функционирует в многопользовательской среде, то помимо простого контроля доступа средства защиты информации от НСД выполняют функции разграничения прав доступа разных пользователей к ресурсам и инфраструктурам АС.

В дополнение к функциям аутентификации средства защиты информации от НСД могут выполнять контроль целостности ресурсов и инфраструктур АС. Контроль целостности может осуществляться либо на основе имитовставки алгоритма ГОСТ 28147-89 [7], либо на основе функции хеширования алгоритма ГОСТ Р 34.11-34. В этом случае средства защиты информации от НСД функционируют аналогично системам обнаружения ВН, базирующимся на методе контроля целостности (см. п. 5.4). Как правило, для повышения производительности средствами защиты информации от НСД осуществляется контроль целостности не всех ресурсов и инфраструктур АС, а лишь их наиболее критических компонентов. Контроль целостности может осуществляться как в процессе загрузки, так и динамически в процессе функционирования АС.

В процессе своего функционирования средства зашиты информации от НСД формируют журнал аудита безопасности, содержащий следующие регистрационные записи:

- дату и время попытки доступа субъектов к ресурсам и инфраструктурам АС с указанием её результата (успешный, неуспешный - несанкционированный);

- идентификатор субъекта, предъявленный при попытке получения доступа;

- аутентификационные параметры субъекта, предъявленные при неуспешной попытке доступа.

# 4. Технология антивирусной защиты

Технология антивирусной защиты представляет собой совокупность методов обнаружения и удаления программных компонентов, несанкционированно внедрённых в информационную сферу АС и предназначенных для выполнения несанкционированных действий, направленных на реализацию угроз ИБ. Такие программные компоненты принято называть «вирусами» [46]. Частными случаями вирусов являются: информационные «закладки», информационные люки, программы типа «троянский конь» и др. Внесение вирусов может осуществляться нарушителем как на техноло­гическом, так и на эксплуатационном этапе жизненного цикла ГСПД.

Технология антивирусной защиты реализуется при помощи специализированного программного обеспечения, называемого антивирусными программами. Существует четыре основных типа антивирусных программ: сканеры, программы контроля целостности данных, мониторы и гибридные антивирусные средства.

Алгоритм работы антивирусного сканера заключается в обнаружении вирусов на базе сигнатур, хранящихся в БД сканера. Сигнатура вируса представляет последовательность кода, характерную для этого вируса. Если в процессе анализа информационных ресурсов и инфраструктур АС на предмет наличия вирусов сканер встретит фрагмент кода, соответствующий сигнатуре, хранящейся в его БД, то он сигнализирует об обнаружении вируса. Недостатком антивирусных сканеров является невозможность обнаружения тех вирусов, которых нет в его БД. Для устранения этого недостатка в сканерах используется дополнительный компонент - эвристический анализатор, предназначенный для обнаружения вирусов, заранее неизвестных сканеру. Однако данный метод обнаружения вирусов является недостаточно надёжным и характеризуется большим количеством ложных срабатываний.

Программы контроля целостности данных предназначены для обнаружения вирусов путём отслеживания изменений, внесённых в информационные ресурсы и инфраструктуры защищаемой АС. Контроль изменений ресурсов и инфраструктур осуществляется при помощи механизма контрольных сумм. Алгоритм работы антивирусных программ этого типа аналогичен работе систем обнаружения ВН. построенных на базе метода контроля целостности.

Антивирусные мониторы - это специальные программы, которые функционируют в фоновом режиме ОС защищаемой АС и осуществляют проверку всех ресурсов и инфраструктур, с которыми работает ОС АС. При этом обнаружение вирусов осуществляется при помощи рассмотренных выше алгоритмов работы антивирусных сканеров.

# Заключение

Информационная безопасность современных автоматизированных систем согласно общепринятому подходу включает три взаимоувязанных аспекта:

• целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения;

• конфиденциальность – защита от несанкционированного ознакомления с информацией;

• доступность – возможность за приемлемое время получить требуемую информацию, информационную услугу.

Наиболее вероятными причинами нарушения доступности информации можно считать следующие:

• отнесение к информации ограниченного доступа информационных ресурсов, которые в соответствии с законодательством РФ являются открытыми;

• локализация информационных ресурсов внутри отдельных подразделений из-за нежелания руководства этих подразделений предоставлять информацию сотрудникам других подразделений, даже в ущерб общему делу;

• увеличение времени отклика системы в связи с недостаточной производительностью программно-технических средств или из-за ненадежности программ или технических средств.

Вопросы информационной безопасности в СД МТ следует решать на основе комплексного учета всех трех названных аспектов. При этом необходимо иметь в виду два существенных фактора:

• действие аспектов целостности и конфиденциальности, с одной стороны, и доступности, с другой стороны, обычно противоположно. Повышение уровня целостности и конфиденциальности практически всегда ведет к увеличению времени реакции системы, дополнительным задержкам информации, то есть к ухудшению доступности. Можно сделать систему, хорошо защищенную от НСД, но совершенно непригодную для работы в режиме, близком к реальному масштабу времени;

• повышение уровня целостности и конфиденциальности, как правило, сопряжено с резким ростом стоимости системы, а это может оказаться практически неприемлемым для СД.

Потребность в защите информации зависит от рода выполняемой вами работы и от чувствительности информации, которой вы управляете. Однако все хотят секретности и чувства безопасности, которое появляется вместе с обоснованной уверенностью в том, что они не могут стать жертвой нарушения защиты информации.

Деятельность организации обеспечивается системой взаимоувязанной управленческой документации. Её состав определяется компетенцией структурных подразделений организации, порядком разрешения вопросов (единоначальный или коллегиальный), объёмом и характером взаимосвязей между организацией и его структурными подразделениями, другими органами управления и организациями.

Процесс выявления и регламентации состава информации – это тайна фирмы, являющаяся основополагающей частью системы защиты информации. Состав этих сведений фиксируется в специальном перечне, где закрепляется факт отнесения их к защищаемой информации и определяющий период конфиденциальности сведений, уровень или гриф секретности, а также список лиц, которые имеют право использовать их сведения.

Ценность информации и требования к её надежности находятся в прямой зависимости. Ценность информации может быть выражена в денежном эквиваленте и характеризовать конкретный размер прибыли при её использовании или размер убытков при её потере. Производственная или коммерческая ценность недолговечна и определяется временем, необходимым конкурентам для выработки той же идеи или её хищения.

Рассмотрение вопросов обеспечения гарантированных качественных характеристик процесса передачи данных ГСПД или качества обслуживания ГСПД в условиях возможных воздействий нарушителя информационным оружием на информационную сферу ГСПД и составляет основу проблемы обеспечения ИБ ТТ.

Внедрение в сетях связи России передовых телекоммуникационных технологий, дает, с одной стороны, существенный эффект в предоставлении пользователям сетей современных услуг связи, а, с другой стороны, создает предпосылки риска блокирования (как правило, в самый не благоприятный момент времени) процесса передачи информации и, как следствие, экономического, социального и других видов ущерба пользователю, оператору связи и государству. Нарушители (злоумышленники), вторгающиеся в работу сетей связи, способны не только добывать циркулирующую в них информацию, но и вводить в средства связи или активизировать в определенные моменты времени уже содержащиеся в средствах связи разрушающие «вирусы» и программные закладки, направленные на нарушение процессов функционирования сетей связи вплоть до полного блокирования процесса передачи информации.

Вскрытие в используемых телекоммуникационных технологиях недостатков (уязвимостей), способствующих успешным воздействиям нарушителя, и принятие активных мер защиты по поддержанию устойчивого функционирования сетей связи в условиях возможных воздействий нарушителя - являются основными задачами при решении проблем обеспечения их информационной безопасности.

Рассмотрение вопросов обеспечения гарантированных качественных характеристик процесса передачи данных ГСПД или качества обслуживания ГСПД в условиях возможных воздействий нарушителя информационным оружием на информационную сферу ГСПД и составляет основу проблемы обеспечения ИБ ТТ.

Решение любой новой проблемы требует предварительного решения как минимум двух задач:

- убедить всю иерархию специалистов и чиновников, связанных с решением этой проблемы, в необходимости ее решения;

- воплотить методологическую основу новой проблемы в механизмы и технологии, создающие необходимый практический базис ее решения.

# Список литературы

1. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
2. Система обеспечения информационной безопасности Взаимоувязанной сети связи Российской Федерации. Термины и определения. Стандарт отрасли. ОСТ 45.127-99.
3. Алгулиев Р.М. Методы синтеза адаптивных систем обеспечения информационной безопасности корпоративных сетей. М.: УРСС, 2001.
4. Белоусов И.В. Информационная безопасность телекоммуникационных сетей: проблемы и пути их решения //Безопасность информационных технологий. 1999. № 1.
5. Бешелев С.Д., Гурвич Р.Г. Математико-статистические методы экспертных оценок. М.: Статистика, 1980 с.
6. Буяльский К.Л., Шахов В.Г. Организация работы удаленных пользователей корпоративной сети в защищенном режиме//Ведомственные корпоративные сети системы. 2001. № 6.
7. Володин А.В., Устинов Г.Н. О гарантированной доставке информации // Документальная электросвязь. 1999. № 1.
8. Володин А.В., Устинов Г.Н. Система защиты пакетов данных в процессе их передачи в выделенном защищаемом фрагменте сети передачи данных общего пользования с коммутацией пакетов от несанкционированных воздействий // Российское агентство по патентам и товарным знакам Свидетельство на полезную модель от 27.02.2001 г. № 16962.
9. Володин А.В., Устинов Г.Н., Алгулиев Р.М. Как обеспечить безопасность сети передачи данных // Технологии и средства связи. 1999. №4.
10. Гриняев С.Н. Интеллектуальное противодействие информационному оружию. М.: Синтег, 1999.
11. Крис Касперски. Техника сетевых атак. М.: СОЛОН-Р, 2001.
12. Кульгин М. Технологии корпоративных сетей. Спб.: Питер, 2000.
13. Лукацкий А. В. Обнаружение атак. Спб.: БХВ-Санкт-Петербург, 2001.
14. Максим Кульгин. Технологии корпоративных сетей. Спб.: Питер, 2000.
15. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Интернет. М: ДМК, 2000.
16. Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений. М.: Юнити, 2001.
17. Новиков А.А., Устинов Г.Н. Защита процесса передачи данных от возможности его блокирования вследствие информационных воздействий нарушителя на информационную сферу сети передачи данных общего пользования -- основная задача обеспечения информационной безопасности ВСС РФ // Тр. 4-го Всероссийского отраслевого совещания «Безопасное функционирование отрасли - составная часть национальной безопасности» Минсвязи России-2001.
18. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Спб.: Питер, 2000.
19. Петраков А. В. Основы практической защиты информации. М: Радио и связь, 2001.368с.
20. Приходько А. Я. Словарь-справочник по информационной безопасности. М.: СИНТЕГ, 2001. 124 с.
21. Приходько А.Я. Информационная безопасность в событиях и фактах. М.: СИНТЕГ. 2001.260с.
22. Скородумов Б.И. Информационная безопасность. Обеспечение безопасности информации электронных банков; Учебное пособие. М.: МИФИ, 1995.
23. Устинов Г.Н.. О проблеме обеспечения информационной безопасности систем и сетей связи // Метрология и измерительная техника в связи. 2000, №3.