ISBN: 978-93-26365-54-5

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: МОДЕЛИРОВАНИЕ КИБЕРАТАКИ НА БАНКОВСКИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

CYBER SECURITY

Author

БЕКБАЕВ ГАМЗАТДИН АЛЕУАТДИНОВИЧ

Published by
Novateur Publication
466, Sadashiv Peth, M.S.India-411030
novateurpublication.org

ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

БЕКБАЕВ ГАМЗАТДИН АЛЕУАТДИНОВИЧ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: МОДЕЛИРОВАНИЕ КИБЕРАТАКИ НА БАНКОВСКИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

МОНОГРАФИЯ

Ташкент 2023 г.

Информационная безопасность: моделирование кибератаки на банковские информационные системы: монография / Г.А. Бекбаев – Ташкент: «Iqtisodchi» ТГЭУ, 2023. – 168 с.

Монография содержит теоретические основы информационного воздействия на элементы банковских информационных систем. Разработаны модели и методики, позволяющие прогнозировать распределение компьютерных атак по элементам, с учетом места и роли элементов в банковской информационной системе, а также определить показатели, характеризующие устойчивость корпоративной сети в условиях воздействия компьютерных атак и требования системе защиты. Полученные результаты позволяют обосновать топологию корпоративных сетей, нейтрализующую сильные стороны компьютерных атак, систему защиты, целью которой является предотвращение (затруднение) реализации компьютерных атак. Обосновывается комплексный подход к обеспечению информационной безопасности корпоративных сетей. Описываются базовые технологии защиты межсетевого обмена данными. Рассматриваются методы и средства антивирусной защиты.

Монография может быть использована в качестве материала лекционных занятий по предмету «Информационная безопасность» для студентов бакалавриата по направлению (60310500 – цифровая экономика).

Рецензенты: Алланов О.М. заведующий кафедрой «Кибербезопасность и криминалистика» ТУИТ

Абдуллаева И.М. доцент кафедры «Искусственный интеллект» ТГЭУ

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В условиях цифровой экономики система расчетов между банками и автоматизации их работы на рынке ценных бумаг, розничных операций (работа банкоматов, терминалов и кредитных карточек), системы автоматизированного взаимодействия является важной функцией банков. Банки уделяют пристальное внимание работе с клиентами через такие программы как «банк-клиент», совершенствуется обмен информацией с филиалами и отделениями расположенных в других городах, а связь с ними обеспечивается с помощью банковских информационных систем (БИС). За последние месяцы текущего года были выявлены несколько кибератак на банковские информационные системы крупнейших банков республики. В частности на БИС “Асакабанк”, “InfinBank” и “Давр банк” [52-54]. В результате кибератак хакеры (злоумышленники) присвоили несколько миллиардов сумов. Таким образом, актуализируется задача научной оценки возможностей злоумышленников по осуществлению кибератак на сетевые элементы БИС банковских сфер Республики Узбекистан.

Новые технологические возможности облегчают распространение информации, повышают эффективность бизнес процессов, способствуют расширению деловых отношений. Однако, несмотря на интенсивное развитие компьютерных средств и информационных технологий, уязвимость современных информационных систем и компьютерных сетей, к сожалению, не уменьшается. Поэтому проблемы обеспечения информационной безопасности привлекают пристальное внимание как специалистов в области информационных технологий и сетей, так и многочисленных пользователей, включая компании, банковско-финансовые организации, работающие в сфере бизнеса.

Данная монография знакомит читателя с основными результатами исследований в области разработки нормативных, теоретических и практических и положений технологии построения специальных

защищенных информационных систем. Представленная в этой монографии постановка задачи построения защищенных банковских информационных систем своей попыткой комплексного решения проблемы является новое направление в области обеспечения безопасности информационных систем и сетей и создания защищенных систем обработки информации.

Автор ставил перед собой задачу ответить основные теоретические аспекты созданы подобных систем и дать ответы на следующие вопросы:

– основные понятия и определения информационной безопасности;

– анализ угрозы кибератаки на банковские информационные системы;

– что представляет собой защищенная система;

– какими должны быть требования к безопасности банковской информационной системе;

– каким образом можно учесть негативный опыт нарушения безопасности существующих банковских информационных систем;

– какие принципы могут быть положены в основу технологии создания защищенных систем обработки информации.

Поэтому все главы данной монографии были направлены пользователям для получения ответов на поставленные вопросы.

ГЛАВА 1. ОСНОВНЫЕ ПОНЯТИЯ И КИБЕРУГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. АНАЛИЗ КИБЕРАТАКИ НА БАНКОВСКИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

1.1. Сущность и основные понятия информационной безопасности.

Новые информационные технологии (ИТ) активно внедряются во все банковские сферы республики. Появление локальных и глобальных сетей передачи данных предоставило пользователям (клиентам) компьютеров новые возможности для оперативного обмена информацией. По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им ИТ. Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий. Рассмотрим основные понятия защиты информации и информационной безопасности компьютерных систем и сетей [2, 27-49]:

Под информационной безопасностью – понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Известно, кибербезопасность является основной составляющей информационной безопасности, в связи, с чем и согласно закону Республики Узбекистан о Кибербезопасности [2] можно дать следующее определение: **кибербезопасность** – состояние защищенности интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве. Также в данном законе даны конкретные определения таких понятий, как:

- **объект информатизации** – информационные системы (технологии) различного уровня и назначения, сети телекоммуникаций, технические средства обработки информации, помещения, где установлены и эксплуатируются эти средства;
- **киберпространство** – виртуальная среда, созданная с помощью информационных технологий;
- **киберугроза** – комплекс условий и факторов в киберпространстве, представляющих угрозу интересам личности, общества и государства;
- **кибератака** – действие, представляющее угрозу кибербезопасности, умышленно осуществляемое в киберпространстве с использованием аппаратных, аппаратно-программных и программных средств;
- **критическая информационная инфраструктура –** комплекс автоматизированных систем управления информационных систем и ресурсов сетей и технологических процессов, имеющих важное стратегическое и социально-экономическое значение;
- **объекты критической информационной инфраструктуры –** системы информатизации применяемые в сфере государственного управления и оказания государственных услуг, обороны, обеспечения государственной безопасности, правопорядка, топливно-энергетического комплекса (атомной энергетики) химической и нефтехимической отраслях, металлургии, водопользования и водоснабжения, сельского хозяйства, здравоохранения, жилищно-коммунального обслуживания, банковско-финансовой системы, транспорта, информационно-коммуникационных технологий, экологии и охраны окружающей среды, добычи и переработки полезных ископаемых стратегического значения, производственной сфере, а также в других отраслях экономики страны.

Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Для более полного раскрытия данного термина необходимо знание следующих терминов:

- **инцидент кибербезопасности** – событие в киберпространстве, приведшее к сбоям в работе информационных систем и (или) нарушениям доступности информации в них, целостности и ее свободного использования;
- **объект кибербезопасности –** комплекс информационных систем, используемых в деятельности по обеспечению киберзащиты информации и кибербезопасности национальных информационных систем и ресурсов, в том числе объекты критической информационной инфраструктуры;
- **субъект кибербезопасности –** юридическое лицо или индивидуальный предприниматель, имеющий определенные права и обязанности, связанные с владением, пользованием и распоряжением национальными информационными ресурсами и оказанием информационных электронных услуг по их использованию, защитой информации и кибербезопасностью, в том числе субъекты критической информационной инфраструктуры;
- **цель защиты информации** – это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию;
- **система защиты информации** – совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации;
- **способ защиты информации** – порядок и правила применения определенных принципов и средств защиты информации;
- **средство защиты информации** – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации;

- **комплекс средств защиты (КСЗ)** – совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности системы (сети). КСЗ создается и поддерживается в соответствии с принятой в данной организации политикой безопасности;

- **киберзащита** – комплекс правовых, организационных, финансово-экономических, инженерно-технических мер, а также мер криптографической и технической защиты данных, направленных на предотвращение инцидентов кибербезопасности, выявление кибератак и защиту от них, устранение последствий кибератак, восстановление стабильности и надежности деятельности телекоммуникационных сетей, информационных систем и ресурсов;

- **политика безопасности** – это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерной системы от заданного множества угроз. Политика безопасности информационных потоков основана на разделении всех возможных информационных потоков между объектами системы на два непересекающихся множества: множество благоприятных информационных потоков и множество неблагоприятных информационных потоков. Цель реализации политики безопасности информационных потоков состоит в том, что бы обеспечить невозможность возникновения в компьютерной системе неблагоприятных информационных потоков;

- **защита информации от утечки** – деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками;

- **защита информации от разглашения** – деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации;

- **защита информации от НСД** – деятельность по предотвращению получения защищаемой информации заинтересованным субъектом, с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим НСД к защищаемой информации, может выступать государство, юридическое лицо группа физических лиц: в том числе общественная организация, отдельное физическое лицо;
- **эффективность защиты информации** – степень соответствия результатов защиты информации поставленной цели.

Современная банковская информационная система (БИС) представляет собой сложную систему, состоящую из большого количества компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты БИС можно разбить на следующие группы:

- **аппаратные средства** – персональные компьютеры и их компоненты, сетевые устройства и линии связи;
- **программное обеспечение** – приобретенные программы: исходные или загрузочные модули; операционные системы и системные программы (компиляторы, утилиты, диагностические программы) и др.

Под угрозой информационной безопасности БИС понимаются возможные действия, способные прямо или косвенно нанести ущерб ее безопасности. Ущерб безопасности подразумевает нарушение состояния защищенности информации, содержащейся и обрабатывающейся в системе БИС. С понятием угрозы безопасности тесно связано понятие уязвимости компьютерной системы.

Информационная безопасность банковских информационных систем (БИС) достигается обеспечением:

- конфиденциальности;

- целостности;
- доступности информационных компонентов и ресурсов системы.

Конфиденциальность данных – это статус, предоставленный данным и определяющий требуемую степень их защиты. К конфиденциальным данным можно отнести, например: личную информацию пользователей (клиентов), учетные записи (имена и пароли), данные о кредитных картах, данные о разработках и различные внутренние документы, бухгалтерские сведения. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам системы. Для остальных субъектов системы эта информация должна быть неизвестной.

Под целостностью информации – понимается свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения. Целостность информации обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении от данных в исходных документах, то есть если не произошло их случайного или преднамеренного искажения или разрушения. Обеспечение целостности данных (информации) является одной из сложных задач защиты информации. Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий). Практически все нормативные документы и отечественные разработки относятся к статической целостности, хотя динамический аспект не менее важен. Статическую целостность можно разделить на понятия целостности данных и целостности информации.

- **целостность данных** – способность данных не подвергаться изменению или аннулированию в результате несанкционированного доступа;
- **целостность информации –** способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Доступность – такое состояние информации, когда она находится в виде и месте, необходимом пользователю, и в то время, когда она ему необходима. Различают санкционированный и несанкционированный доступ к информации:

- **санкционированный доступ к информации** – это доступ к информации, не нарушающий установленные правила разграничения доступа;
- **несанкционированный доступ к информации** – нарушение установленных правил разграничения доступа. Лицо или процесс, осуществляющие НСД к информации, являются злоумышленниками правил разграничения доступа. С доступом к информации и ресурсам системы связана группа таких важных понятий, как:
- идентификация;
- аутентификация;
- авторизация.

Идентификация – это процедура распознавания субъекта по его идентификатору. Идентификация выполняется при попытке субъекта войти в систему (сеть).

Аутентификация – это проверка подлинности субъекта с данным идентификатором. Процедура аутентификации устанавливает, является ли субъект именно тем, кем он себя объявил.

Авторизация – предоставление определенному лицу прав на выполнение определенных действий.

Уязвимость компьютерной системы – это присущее системе неудачное свойство, которое может привести к реализации угрозы.

Атака на компьютерную систему (сеть) – это поиск и/или использование злоумышленником той или иной уязвимости системы. Иными словами, атака – это реализация угрозы безопасности. Противодействие угрозам безопасности является целью средств защиты компьютерных систем и сетей.

1.2. Угрозы информационной безопасности. Киберугрозы. Сегодня в целях обеспечения максимальной эффективности деятельности банковских сфер в его информационной инфраструктуре применяются современные информационно-коммуникационные технологии. Наряду с неоспоримыми преимуществами применения современных информационных технологий существуют риски реализации угроз информационной безопасности, последствием которой может стать нарушение функционирования Центрального банка Республики Узбекистан и его все структурные подразделения.

Под угрозой понимают потенциально возможное событие (воздействие, процесс или явление), которое может привести к нанесению ущерба чьим-либо интересам. В настоящее время известен обширный перечень угроз информационной безопасности автоматизированных систем, содержащий сотни позиций. Рассмотрение возможных угроз информационной безопасности проводится с целью определения полного набора требований к разрабатываемой системе защиты. Перечень угроз, оценки вероятностей их реализации, а также модель злоумышленника служат основой для анализа риска реализации угроз и формулирования требований к системе защиты банковских информационных систем. Кроме выявления возможных угроз, целесообразно проведение анализа этих угроз на основе их классификации по ряду признаков. Каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. Угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование.

Необходимость классификации угроз информационной безопасности обусловлена тем, что информация, хранящаяся и обрабатываемая в современных банковских информационных системах, подвергается воздействию чрезвычайно большого количества факторов, что не позволяет формализовать задачу описания полного набора угроз. Классификация

возможных угроз информационной безопасности БИС может быть проведена по следующим базовым признакам:

По природе возникновения:

- естественные угрозы – вызванные воздействиями на БИС объективных физических процессов или стихийных природных явлений;
- искусственные угрозы – вызванные воздействием на БИС человеческой деятельностью.

По степени преднамеренности проявления:

- угрозы, вызванные ошибками или халатностью персонала, например некомпетентное использование средств защиты, ввод ошибочных данных и т.п.;
- угрозы преднамеренного действия, например действия злоумышленников.

По непосредственному источнику угроз:

- природная среда – например, стихийные бедствия, магнитные бури и пр.;
- человек – например, вербовка путем подкупа персонала, разглашение конфиденциальных данных и т.п.;
- санкционированные программно-аппаратные средства – например, удаление данных, отказ в работе операционной системы;
- несанкционированные программно-аппаратные средства – например, заражение компьютера вирусами с деструктивными функциями.

По положению источника угроз:

- вне контролируемой зоны БИС – например, перехват данных, передаваемых по каналам связи, перехват побочных электромагнитных, акустических и других излучений устройств;
- в пределах контролируемой зоны БИС – например, применение подслушивающих устройств или хищение: записей, носителей информации и т.п.;

- непосредственно в БИС – например, некорректное использование ресурсов или программного обеспечения БИС.

По степени зависимости от активности БИС:

- независимо от активности БИС – например, вскрытие шифров криптозащиты информации;
- только в процессе обработки данных – например, угрозы выполнения и распространения программных вирусов.

По степени воздействия на БИС:

- пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании БИС, например, угроза копирования секретных данных;
- активные угрозы, которые при воздействии вносят изменения в структуру и содержание БИС, например, внедрение троянских коней и вирусов.

По этапам доступа пользователей или программ к ресурсам БИС:

- угрозы, проявляющиеся на этапе доступа к ресурсам БИС – например, угрозы несанкционированного доступа в БИС;
- угрозы, проявляющиеся после разрешения доступа к ресурсам БИС – например, угрозы несанкционированного или некорректного использования ресурсов БИС.

По способу доступа к ресурсам БИС:

- угрозы, осуществляемые с использованием стандартного пути доступа к ресурсам БИС – например, незаконное получение паролей и других реквизитов разграничения доступа с последующей маскировкой под зарегистрированного пользователя;
- угрозы, осуществляемые с использованием скрытого нестандартного пути доступа к ресурсам БИС – например, несанкционированный доступ к ресурсам БИС путем использования недокументированных возможностей операционных систем.

По текущему месту расположения информации, хранимой и обрабатываемой БИС:

- угрозы доступа к информации, находящейся на внешних запоминающих устройствах – например, несанкционированное копирование секретной информации с жесткого диска;
- угрозы доступа к информации, находящейся в оперативной памяти – например, чтение остаточной информации из оперативной памяти, доступ к системной области оперативной памяти со стороны прикладных программ;
- угрозы доступа к информации, циркулирующей в линиях связи – например, незаконное подключение к линиям связи с последующим вводом ложных сообщений или модификацией передаваемых сообщений, незаконное подключение к линиям связи с целью прямой подмены законного пользователя с последующим вводом дезинформации и навязыванием ложных сообщений;
- угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере, например запись отображаемой информации на скрытую видеокамеру.

Киберугроза – это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных, целей. Киберугроза может воздействовать на информационное пространство банковских информационных систем. В настоящее время известен обширный перечень угроз информационной безопасности БИС, содержащий сотни позиций. Рассмотрение возможных угроз информационной безопасности проводится с целью определения полного набора требований к разрабатываемой системе защиты. Перечень угроз, оценки вероятностей их реализации, а также модель злоумышленника служат основой для анализа риска реализации угроз и формулирования требований к системе защиты БИС. Кроме выявления возможных угроз, целесообразно проведение анализа этих угроз на основе их классификации отражает одно из обобщенных требований к системе защиты. Угрозы,

соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование. Киберугроза реализуется в виде атаки, в результате чего и происходит нарушение безопасности информации. Целесообразно выделить следующие основные виды нарушения безопасности информации:

- нарушение конфиденциальности;
- нарушение целостности;
- нарушение доступности.

Угрозы нарушения конфиденциальности – направленные на разглашение конфиденциальной или секретной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ.

Угрозы нарушения целостности информации – хранящейся в компьютерной системе или передаваемой по каналу связи, которые направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению. Целостность информации может быть нарушена умышленно, а также в результате объективных воздействий со стороны среды, окружающей систему.

Угрозы нарушения доступности – направленные на создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность банковских информационных систем, либо блокируют доступ к некоторым ее ресурсам.

В таблице 1.1 приведены некоторые виды киберугрозы информационной безопасности, а также возможные последствия от их реализации. Следует отметить, что чаще всего для достижения поставленной цели злоумышленник реализует не одну, а некоторую совокупность из этих кибератак. Важность того или иного вида нарушения безопасности зависит от многих факторов. Например, для подчеркнуто открытой организации может просто не существовать угроз конфиденциальности – вся информация считается общедоступной.

Таблица 1.1 – Киберугрозы и последствия от их реализации

Виды киберугрозы	**Возможные последствия нарушения:**		
	Конфиденциальности	**Целостности**	**Доступности**
Подключение к каналам связи	да	да	да
Пассивный перехват информации в сети	да	нет	нет
Активный перехват информации в сети	да	да	да
Изменение протокола обмена	да	да	да
Изменение потока сообщений	да	да	да
Установление незаконного соединения в сети	да	да	да
Изменение полномочий других пользователей в сети	да	да	да
Маскировка под шлюз	да	да	да
Использование терминальных серверов для маскировки	да	да	да
Пересылка информации по ошибочному адресу	да	да	да
Нарушение целостности электронного письма	нет	да	да
Разглашение атрибутов разграничения доступа (паролей, шифров и др.)	да	да	да
Незаконное получение атрибутов разграничения доступа	да	да	да
Вскрытие шифров криптозащиты	да	нет	нет
Нарушение процесса криптозащиты	да	да	да
Внесение изменений в программы системы защиты	да	да	да
Обход системы защиты	да	да	да

Отключение системы защиты	да	да	да
Отключение криптозащиты	да	да	нет
Нарушение установленных правил при работе в системе	да	да	да
Изменение программ	да	да	да
Удаление программ	нет	да	да
Изменение режимов работы программного обеспечения	да	да	да
Ввод ошибочной информации	нет	да	да
Копирование информации с машинных носителей	да	нет	нет
Незаконное использование «точек входа»	да	да	да
Использование неправильно спроектированных программ	да	да	да
Использование программ с ошибками	да	да	да
Использование неучтенных (незаконных) программ	да	да	да
Неправомерная перегрузка (компонентов системы)	нет	да	да
Ошибка при использование языков доступа к данным (SQL)	да	да	да
Внедрение вирусов	да	да	да
Атака хакеров	да	да	да

Угрозы могут быть преднамеренными или непреднамеренными (случайными). Причинами случайных воздействий при эксплуатации БИС могут быть:

– аварийные ситуации из-за стихийных бедствий и отключений электропитания;

– отказы и сбои аппаратуры;

– ошибки в программном обеспечении (ПО);

– ошибки в работе обслуживающего персонала и пользователей;

– помехи в линиях связи из-за воздействий внешней среды.

Ошибки в ПО являются распространенным видом компьютерных нарушений. ПО серверов, рабочих станций, маршрутизаторов и т.д. написано людьми, поэтому оно практически всегда содержит ошибки. Чем выше сложность подобного ПО, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляют никакой опасности, некоторые же могу привести к серьезным последствиям, таким как получение, злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов. Обычно подобные ошибки устраняются с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких пакетов является необходимым условием безопасности информации.

Преднамеренные угрозы связаны с целенаправленными действиями злоумышленника. В качестве злоумышленника может быть служащий, посетитель, конкурент, наемник и т.д. Действия злоумышленника могут быть обусловлены разными мотивами:

– недовольством служащего своей карьерой;

– сугубо материальным интересом (взятка);

– любопытством;

– конкурентной борьбой;

– стремлением самоутвердиться любой ценой и т.п.

В частности, для банковских информационных систем можно выделить следующие преднамеренные угрозы:

– НСД лиц, не принадлежащих к числу банковских служащих, и ознакомление с хранимой конфиденциальной информацией;

– хищение денег у клиентов с использованием вредоносных программ;

– ознакомление банковских служащих с информацией, к которой они не должны иметь доступ;

– шпионаж, кража и публикация информации о VIP-клиентах, их транзакциях;

– несанкционированное копирование программ и данных;

– кража магнитных носителей содержащих конфиденциальную информацию;

– кража распечатанных банковских документов;

– умышленное уничтожение информации;

– несанкционированная модификация банковскими служащими финансовых документов, отчетности и баз данных;

– фальсификация сообщений, передаваемых по каналам связи;

– отказ от авторства сообщения, переданного по каналам связи;

– отказ от факта получения информации;

– навязывание ранее переданного сообщения;

– разрушение информации, вызванное вирусными воздействиями;

– разрушение архивной банковской информации, хранящейся на магнитных носителях.

В таблице 1.2 перечислены основные методы реализации угроз информационной безопасности.

Таблица 1.2 – Основные методы реализации угроз информационной безопасности

Уровень доступа к информации в БИС	**Угроза раскрытия параметров системы**	**Угроза нарушения конфиденциальности**	**Угроза нарушения целостности**	**Угроза отказа служб (отказа доступа к информации)**
Уровень носителей информации	Определение типа и параметров носителей информации	Хищение (копирование) носителей информации	Уничтожение машинных носителей информации	Выведение из строя машинных носителей информации
Уровень средства взаимодействия с носителем	Получение информации о программно-аппаратной среде	Несанкционированный доступ к ресурсам БИС	Внесение пользователем несанкционированных изменений в программы и данные	Проявление ошибок проектирования и разработки программно-аппаратных компонент БИС
Уровень представления информации	Определение способа представления информации	Визуальное наблюдение, раскрытие представления информации (дешифрование)	Внесение искажения в представление данных, уничтожение данных	Искажение соответствия синтаксических и семантических конструкций языка
Уровень содержания информации	Определение содержания данных на качественном уровне	Раскрытие содержания информации	Внедрение дезинформации	Запрет на использование информации

1.3. Анализ кибератаки на банковские информационные системы. **Кибератаки на банковско-финансовую систему США**: 1 ноября 2022 года Агентство по борьбе с финансовыми преступлениями США (FinCEN), входящее в состав Министерства финансов, раскрыло масштабы выплат, которые банки страны осуществили в результате атак программ-вымогателей. Общая сумма превышает $1,2 млрд. В 2021 году финансовые учреждения США зарегистрировали 1489 инцидентов, связанных с атаками, в ходе которых киберпреступники пытались получить выкуп от своих жертв. Для сравнения: в 2020 году было зафиксировано 487 подобных инцидентов. Таким образом, интенсивность атак данного типа увеличилась в три раза. FinCEN заявляет, что программы-вымогатели продолжают представлять серьезную угрозу для критических важных секторов инфраструктуры США, предприятий и рядовых граждан. В марте 2022 года президент США Джо Байден подписал закон о кибербезопасности, который обязывает определенные компании и организации сообщать об инцидентах в Министерство внутренней безопасности в течение 72 часов после обнаружения вторжения и в течение 24 часов, если совершен платеж по требованиям вымогателей [50].

Кибератаки на банковско-финансовую систему Испании: Сотрудники испанских правоохранительных органов арестовали 16 человек, связанных с использованием банковских троянов Mekotio&Grandoreiro в рамках вредоносной кампании, нацеленной на финансовые учреждения в Европе. Об этом стало известно 15 июля 2021 года. Доходы преступников составили 276470 евро. Кибермошенники отправляли потенциальным жертвам фишинговые электронные письма якобы от имени легитимных служб доставки и государственных органов, таких как Казначейство Испании. В письмах пользователей просили перейти по ссылке, которая незаметно загружала вредоносное программное обеспечение на компьютерную систему. Вредоносное программное обеспечение Mekotio&Grandoreiro позволяет перехватывать транзакции на web-сайте

банка и несанкционированно перенаправлять средства на счета, находящиеся под контролем злоумышленников. Для осуществления мошеннических целей преступники взломали, по меньшей мере, 68 учетных записей электронной почты, принадлежащих официальным органам. Это программное обеспечение позволяет похищать пароли из браузеров и памяти устройства, обеспечивая удаленный доступ к операциям Internet-банкинга [50].

Кибератаки на банковско-финансовую систему Южной Кореи: Власти Южной Кореи заявили о кибератаках, которые совершены на десятки правительственных сайтов страны, а также сайты крупных компаний. DDoS-атаки были совершены 4 марта 2022. Атакам подверглась 40 сайтов, в частности сайт президентского Голубого дома, официальные сайты Министерства иностранных дел и Минобороны, а также web-страницы налоговой инспекции. Кроме того, атаке подверглись онлайн-представительства семи крупнейших банков страны. Как сообщалось ранее, 20 марта 2022 компьютерной атакой были полностью парализованы компьютерные сети крупнейших банков Южной Кореи Shinhan, HongHyup и Jeju. Кибератака также нанесли серьезный ущерб, серверам основных телекомпаний, включая государственную телерадиокорпорацию KBS, частный телеканал MBC и новостной канал YTN [51].

Кибератаки на банковско-финансовую систему России: В 2022 году наблюдался существенный рост хакерских атак на инфраструктуру российских банков. Хакеры похитили у клиентов российских банков в 2022 году почти 4 млрд. рублей. Представитель Банка России в разговоре с «Ведомостями» пояснил, что случаи кражи денежных средств в банков в 2022 году были связаны с уязвимостями объектов информатизации и несовершенством бизнес-процессов. По оценке «РТК-Солар», основной угрозой для финансовой отрасли являются высококвалифицированные хакерские группировки, так как, например банков и других крупных финансовых организаций обычно хорошо защищен и для его взлома нужны определенные технические знания и крупные финансовые вложения [55, 56].

Кибератаки на банковско-финансовую систему Узбекистана: В 2022 году были выявлены несколько кибератаки на банковские информационные системы крупнейших банков Республики Узбекистан. В частности на БИС “Асакабанк”, “InfinBank” и “Давр банк”. Хакеры совершили кибератаки на БИС «Асакабанк», и выкрали $700 тыс. со счетов банка [52]. 3-5 сентября 2022 года группе международных финансовых мошенников удалось перевести средства в иностранной валюте из фиктивных торговых сервисов, расположенных за границей, на карты VISA, открытие на имя своих криминальных преступных партнеров в InfinBank, и в эти же дни обналичить их в банкомате через мобильные приложения других банков, посредством карт открытых в системах Humo и Uzcard. В результате хакеров присвоили около $2 млн.[53]. В 2022 году в Ташкенте несколько человек взломали БИС “Давр банк” и перечислили на свои карты 15 млрд. сумов [54]. Сегодня разовые организационно-технические мероприятия по кибербезопасности не могут обеспечить надежной защиты от угроз кибербезопасности в течение продолжительного функционирования. Это связано с постоянным развитием информационной инфраструктуры, изменением методов и способов реализации кибератак, используемых злоумышленниками (киберпреступниками), целью которых является нарушение того или иного технологического процесса, создание финансового и геополитического ажиотажа, а также использование уязвимых информационных узлов (пространств) террористическими группировками – это особо отметил глава государства Мирзияев Ш. М. в ходе Шанхайского саммита в Астане [1]. Во всех вышеперечисленных случаях кибератаки осуществлялись в виде программно-аппаратных воздействий. В работах [6-26] подробно описаны основные виды кибератак (в виде компьютерных атак) на информационно-вычислительную сеть (ИВС) и сеть связи. Анализируя эти работы, можно выделить основные виды компьютерных атак (таблица 1.3).

Таблица 1.3 – Виды компьютерных атак и их возможные последствия

Тип компьютерных атак (КА)	**Способ реализации КА**	**Область проявления**	**Возможные последствия**
Анализ сетевого трафика	- анализ пакетов данных на канальном уровне; - анализ пакетов данных на сетевом уровне	Канал связи	Перехват передаваемых данных, с возможностью определения идентификаторов пользователей и паролей, а также других характеристик сетевого трафика
Сканирование сети и ее уязвимостей	- сканирование пакетом TCP с флагом SYN; - сканирование пакетом TCP с флагом FIN; - сканирование пакетом TCP с флагом ACK; - сканирование пакетом TCP с флагом XMAS; - сканирование пакетом UDP	Коммутатор, маршрутизатор, ПЭВМ, серверы	Определение открытых портов, протоколов взаимодействия, задействованных сетевых служб, идентификаторов пользователей
Взлом паролей	- вирусы изменения системных файлов; - аппаратные закладки; - метод перебора данных в файлах SAM и SYSTEM; - программа сброса паролей; - программа взлома паролей; - программные закладки	Коммутатор, маршрутизатор, ПЭВМ, серверы	Деструктивные действия при получении несанкционированного доступа

Ввод ложной информации, проникновение в специальные базы данных и размещение ложной информации		- аппаратные закладки; - программные закладки; - средства удаленного; администрирования; - вирусы	ПЭВМ, серверы	Изменение маршрутизации данных, навязывание ложной информации, несанкционированный доступ к сетевым ресурсам
Отказ в обслуживание	Локальный отказ в обслуживании	- «тяжелый пакет»; - Mac-flooding	Коммутатор, маршрутизатор, ПЭВМ, серверы	Снижение пропускной способности каналов связи
	Удаленный отказ в обслуживании	- Smurf; - Fraggle; - SYN-flooding		утствие возможности передачи данных в связи с недоступностью среды передачи данных и как следствие – отказ в установлении соединения
	Спам	Рассылка большого числа пакетов сообщений	ПЭВМ, серверы	Снижение производительности сетевых устройств и серверных приложений в результате резкого роста входящего трафика и переполнения буфера
	Логическое отключение абонентов	Перехват IP	ПЭВМ	Разрыв соединения в связи с нарушенной логикой маршрутно-адресных пространств

Классификация кибератак по уровням иерархической модели OSI:

кибератаки на физическом уровне (Physical layer) – кибератаки на физическом уровне известны давно, и, казалось бы, все знают, как с ними бороться, однако иногда и с помощью такой атаки можно получить конфиденциальную информацию. Начнем с простейших сетевых устройств – концентраторов (hub). Как известно, концентратор, получая пакет на один из своих портов, ретранслирует его на все остальные порты (рис.1.1).

Рисунок 1.1 – Внешний вид концентратора и подключение к нему ПК

При этом все персональные компьютеры (ПК), подключенные к данному концентратору, получают отправленный пакет. При использовании этих устройств существенно снижается пропускная способность сегмента сети, и, что гораздо важнее с точки зрения информационной безопасности, любой подключенный к концентратору пользователь может без труда прослушать весь трафик, проходящий через данный сегмент. Для того чтобы проверить это на практике, достаточно подключить к концентратору несколько машин, и на одной из них запустить загрузочный диск и описанный в приложениях дистрибутив Kali или любой другой дистрибутив Linux содержащий данную утилиту. Конечно, многие web-сайты используют шифрование при передаче учетных данных, но тем не менее с помощью прослушивания трафика опытный хакер может собрать массу полезной информации. Например, по тем серверам, к которым обращается компьютер,

можно попытаться определить операционную систему, установленную на компьютере, вплоть до версий установленных обновлений. Также можно узнать об установленных приложениях. Подобные атаки называются «passive fingerprint». Полученная таким образом информация может быть впоследствии использована злоумышленником для реализации более сложных атак.

кибератаки на канальном уровне (Data link layer) – на этом уровне арсенал злоумышленника уже значительно расширяется, и системному администратору нужно принять целый ряд мер для защиты корпоративной сети. Коммутатор (switch) является более интеллектуальным устройством, чем концентратор. Получая пакет на один из своих портов, он, в отличие от концентратора, не пересылает его на все порты, а пересылает только на тот порт, к которому подключен получатель пакета (рис.1.2).

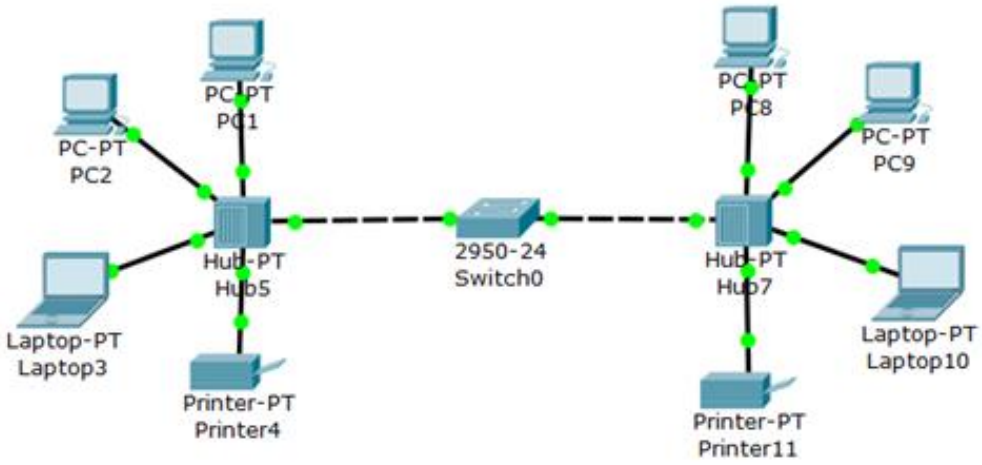

Рисунок 1.2 – Топология сети с коммутатором

На канальном уровне возможны следующие типы атак:

– переполнение CAM-таблицы;

– VLAN Hopping;

– атака на STP;

– MAC- spoofing;

– атака на PVLAN;

– атака на DHCP.

Переполнение CAM-таблицы. Каждый коммутатор имеет CAM-таблицу (Content Address Memory), где содержится привязка MAC-адресов (Media Access Control) к портам коммутатора. То есть в данной таблице указано, какие MAC-адреса, на каком порту принимаются. CAM-таблица имеет ограниченный размер, например коммутатор Cisco Catalyst 2950-24 таблица может хранить до 8000 MAC-адресов. В случае если таблица будет полностью занята, новые записи не смогут добавляться, и весь трафик будет приходить на все порты. Тогда коммутатор начнет работать как обычный концентратор, и весь трафик, проходящий через данный сегмент сети, можно будет прослушать с помощью утилиты Wireshark. Конечно, прослушать весь трафик в локальной сети злоумышленнику таким способом не удастся, но инсайдер, работающий в одном сегменте сети, к примеру с бухгалтерией, сможет перехватывать трафик и получить конфиденциальную информацию. Реализовать данную атаку можно с помощью утилиты macchanger, которая позволяет менять MAC-адреса.

VLAN Hopping. С помощью данной атаки злоумышленник может попытаться передать данные в другой VLAN (Virtual Local Area Network). Как известно, для взаимодействия между виртуальными локальными сетями VLAN в коммутаторах используется режим «mode trunk». В коммутаторах Cisco Catalyst 2950-24 по умолчанию порт работает не в режиме «mode access» и не в режиме «mode trunk», таким образом, на порту работает протокол DTP (Dynamic Trunk Protocol). Очевидно, что при такой настройке портов коммутатора злоумышленнику достаточно притвориться коммутатором, как между ними будет установлено транковое соединение и, соответственно, будут доступны VLAN, сконфигурированные на коммутаторе, после чего передать данные в другой VLAN не ставит труда.

Атака на STP. Протокол STP (Spanning Tree Protocol) предназначен для предотвращения зацикливания пакетов в сети при наличии дублирующих маршрутов. Работает это следующим образом. Сначала производится обнаружение коммутаторов, которые связаны между собой. Затем

выбирается Root Bridge, главный, корневой коммутатор. Далее по специальному алгоритму будут заблокированы порты коммутатора, которые создают петли в получившейся топологии. Для построения древовидной структуры сети без петель в сети должен быть определен корневой коммутатор (root switch), от которого и строится это дерево. В качестве корневого коммутатора выбирается коммутатор с наименьшим значением идентификатора. Идентификатор коммутатора – это число длиной восемь байт, шесть младших байтов которого составляет MAC-адрес его блока управления, а два старших байта конфигурируются вручную. Это позволяет администратору сети влиять на процесс выбора корневого коммутатора. Если администратор не вмешается в этот процесс, корневой коммутатор будет выбран случайным образом, им станет устройство с минимальным MAC-адресом блока управления. Такой выбор может оказаться далеко не рациональным. Поэтому следует выбрать корневой коммутатор, исходя из имеющейся топологии сети, и назначить ему вручную наименьший идентификатор. При автоматическом выборе корневым становится коммутатор с меньшим значением MAC-адреса его блока управления. Далее для каждого коммутатора определяется корневой порт (root port) – этот порт, который имеет по сети кратчайшее расстояние до корневого коммутатора. Для каждого логического сегмента сети выбирается так называемый назначенный мост (designated bridge), один из портов которого будет принимать пакеты от сегмента и передавать их в направлении корневого моста через корневой порт данного моста.

MAC - spoofing. Данный тип атак реализуется путем подделывания MAC-адреса, например атакующий может подделать MAC-адрес, который использовал другой хост сети. Злоумышленник может использовать эту атаку для осуществления сбора конфиденциальной информации. Для реализации данной атаки, как и в предыдущих примерах, можно воспользоваться утилитой macchanger. В результате MAC-адрес указанного сетевого адаптера будет на случайное значение. Для того чтобы предотвратить данный тип

атаки, необходимо выполнить меры, то есть необходимо указать максимальное количество MAC-адресов на порту, указать действие, которое будет выполнено в случае нарушения политики безопасности.

Атака на PVLAN. С помощью этой атаки злоумышленник может получить доступ к соседнему устройству PVLAN посредством L3 устройства (маршрутизатора). В технологии PVLAN, в отличие от VLAN, порты могут находиться в трех режимах: Isolated, Promiscuous, Community. Isolated-порты не могут передавать данные в своем канале VLAN между клиентами. Данные могут передаваться только между портами Isolated и Promiscuous. Порты Promiscuous – это порты PVLAN, в которые можно передавать данные со всех портов Isolated и Community, как и в обычном VLAN. Community – это группы портов, между членами которых можно передавать данные VLAN to VLAN. Если атакующему доступно устройство Layer3 (например, маршрутизатор), он может установить связь между клиентами, которые находятся в одном PVLAN, между портами Isolated. Для реализации данной атаки пользователь может подделать пакет, в котором он укажет в IP-адресе назначения необходимое ему устройство, находящееся на другом порту Isolated, источник останется без изменения, а вот в качестве MAC-адреса назначения он укажет MAC-адрес устройства L3 (layer 3). Данное устройство, получив пакет, переправит его по указанному адресу. Принимающая сторона может сделать то же самое и таким образом обеспечить передачу данных между Isolated-портами.

Атака на DHCP. Атаковать DHCP-сервер можно несколькими различными способами:

– злоумышленник может сформировать и послать DHCP-серверу огромное количество DHCP-запросов с разными MAC-адресами. Сервер будет выделять IP-адреса из пула, и рано или поздно весь DHCP-пул закончится, после чего сервер не сможет обслуживать новых клиентов. По сути, это DoS (Denial of Service)-атака, так как нарушается работоспособность сети. Метод борьбы с подобными атаками называется

DHCP Snooping. Данный метод заключается в следующем. Когда коммутатор получает пакет, то он сравнивает MAC-адрес, указанный в DHCP-запросе, с MAC-адресом, который был прописан на порту коммутатора. Если адреса совпадают, то коммутатор отправляет пакет дальше, если не совпадают, то пакет отбрасывается;

– злоумышленник может также развернуть свой DHCP-сервер и выдавать свои настройки пользователям сети (может указать любой DNS, Gateway и т.д.) и воспользоваться уже по своему усмотрению, начиная от прослушивания трафика до подделки DNS-ответов и т.д.

кибератаки на сетевом уровне (Network layer) – говоря о безопасности на сетевом уровне, необходимо поговорить о маршрутизаторах и алгоритмах маршрутизации. Маршрутизатором является устройство сетевого уровня модели OSI. Это устройство использует одну или более метрик для определения оптимального пути передачи сетевого трафика на основании информации сетевого уровня. Метрики измеряются в количестве переходов, которые необходимо сделать пакету между различными сетями для достижения узла назначения. Из этого определения вытекает, что маршрутизатор, прежде всего, необходим для определения дальнейшего пути данных, посланных в большую и сложную сеть. Пользователь такой сети отправляет свои данные в сеть и указывает адрес своего абонента. Данные проходят по сети и в точках с разветвлением маршрутов поступают на маршрутизаторы, которые как раз и устанавливаются в таких точках. Маршрутизатор выбирает дальнейший наилучший путь. То, какой путь лучше, определяется количественными показателями, которые называются метриками. Лучший путь – это путь с наименьшей метрикой. В метрике может учитываться несколько показателей, например длина пути, время прохождения и т.д.

Существует несколько способов реализации маршрутизаторов. Маршрутизаторы бывают верхнего, среднего и нижнего классов. Маршрутизаторами верхнего класса являются высокопроизводительные

устройства, которые служат для объединения сетей предприятия. Они поддерживают множество протоколов и интерфейсов (рис.1.3).

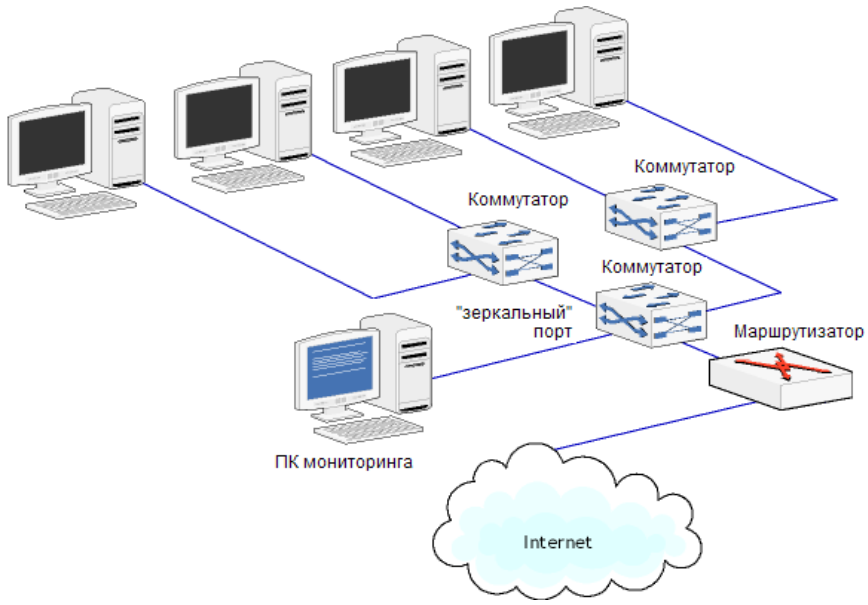

Рисунок 1.3 – Топология сети с маршрутизатором

Маршрутизаторы данного типа могут иметь до нескольких портов локальных или глобальных сетей. Маршрутизаторы среднего класса используются для формирования менее крупных сетевых объединений масштаба предприятия. Стандартная конфигурация таких устройств включает два-три порта локальных сетей и от четырех до восьми портов глобальных сетей. Такие маршрутизаторы поддерживают наиболее распространенные протоколы маршрутизации и транспортные протоколы. Устройства маршрутизации нижнего класса предназначаются для локальных сетей подразделений они связывают небольшие офисы и филиалы с сетью предприятия. Типичная конфигурация включает один порт локальной сети (как правило, Ethernet) и два порта глобальной сети, рассчитанные на низкоскоростные выделенные линии или коммутируемые соединения.

По определению, основное назначение маршрутизаторов – это маршрутизация трафика сети. Основным результатом работы алгоритма маршрутизации являются создание и поддержка таблицы маршрутизации, в которую записывается вся маршрутная информация. Содержание таблицы

маршрутизации зависит от используемого протокола маршрутизации. В общем случае таблица маршрутизации содержит следующую информацию:

– действительные адреса устройств в сети;

– служебную информацию протокола маршрутизации;

– адреса ближайших маршрутизаторов.

Основными требованиями, предъявляемыми к алгоритму маршрутизации, являются:

– оптимальность выбора маршрута;

– простота реализации;

– устойчивость;

– быстрая сходимость;

– гибкость реализации.

Для небольших и статических объединенных IP-сетей с единственными путями подходит среда со статической IP-маршрутизацией. Статическими являются сети, которые не изменяются. На практике статическая маршрутизация обычно встречается в домашних сетях и сетях небольших компаний, до 20 пользователей. Дешевые маршрутизаторы, как правило, поддерживают только статическую маршрутизацию.

В средах с динамической маршрутизацией необходимо больше внимания уделять вопросам безопасности, так как здесь угроз значительной больше, чем в статической среде. Статическая маршрутизация хорошо в небольших сетях, где нет большого количества маршрутов. В случае если сеть состоит из нескольких сегментов, в каждом из которых возможно несколько маршрутов, то здесь использовать статические маршруты будет сложны. В случае выхода из строя одного из каналов связи маршруты не изменятся автоматически, и для переключения на другой маршрут необходимо будет вмешательство администратора. При использовании динамической маршрутизации пересчет таблицы маршрутизации произойдет автоматически.

Scapy – универсальное средство для реализации сетевых атак. Это гибкая и функциональная утилита написана на языке Python. Она предназначена для осуществления манипуляций с сетевыми пакетами. С ее помощью можно собрать IP-пакет нужной структуры, необходимой для проведения сетевых атак (рис.1.4).

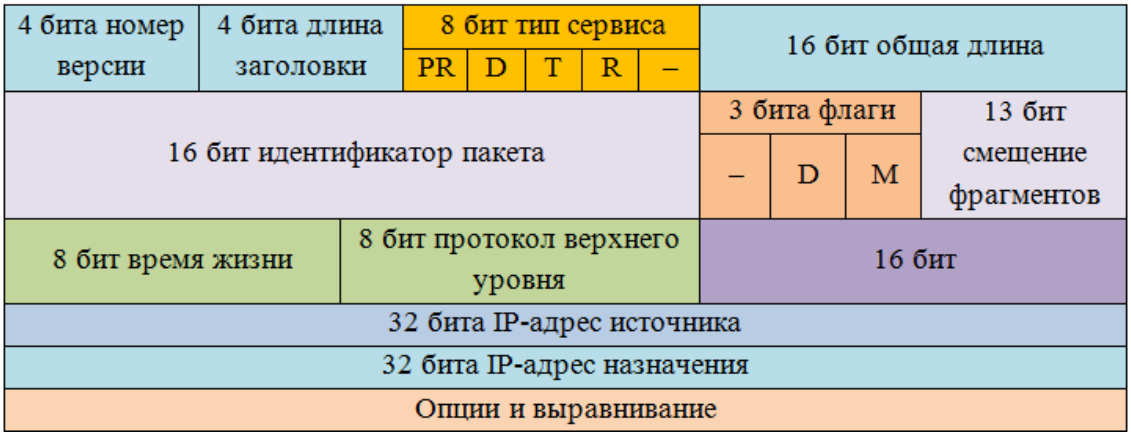

Рисунок 1.4 – Структура IP-пакета

Как известно, стек TCP/IP в различных операционных системах строится на соответствии стандартам RFC, определяющим сетевое взаимодействие. Но для проведения различных атак создаваемые пакеты не всегда должны полностью соответствовать стандартам RFC. Scapy это не только средство для реализации атак на отказ в обслуживании. С помощью данной утилиты можно сконструировать любой пакет с нужными полями и содержимым.

Среды с протоколом RIP. Протокол динамический маршрутизации RIP (Routing Information Protocol) лучше всего подходит для IP-сетей небольших и средних размеров с множественными путями. Термин «сеть с множественными путями» в данном случае означает, что передача пакетов между любыми двумя конечными точками объединенной сети возможна по нескольким различным маршрутам. Протокол маршрутной информации RIP является внутренним протоколом маршрутизации дистанционно-векторного типа. Будучи одним из наиболее ранних протоколов обмена маршрутной информацией, он до сих пор чрезвычайно распространен в локальных сетях

ввиду простоты реализации. У протокола маршрутизации RIP есть еще одно, существенное ограничение. Расстояние между любыми двумя узлами в сети не должно превышать 15 транзитных узлов, в противном случае узел будет считаться недостижимым. Как правило, даже небольшая корпоративная сеть, имеющая несколько филиалов, может столкнуться с этим ограничением при использовании RIP. Основными угрозами для протокола маршрутизации RIP являются:

- ложные маршруты RIP;
- понижение версии протокола RIP;
- взлом хэша MD5;
- слепые DoS-атаки на BGP-маршрутизаторы;
- атака на BGP.

Говоря об угрозах протоколу динамической маршрутизации, стоит прежде всего вспомнить классические атаки, такие как различные виды DDoS (Distributed Denial of Service), а также прослушивание и модификацию трафика. Протокол RIP использует UDP на транспортном уровне и пори 520. Обмен информацией о маршрутах производится через каждые 30 секунд. Соответственно, любая низкоуровневая атака на канал связи между маршрутизаторами приведет к тому, что в течение максимум минуты маршрутизаторы, не сумев обменяться маршрутными таблицами, начнут сообщать о недосягаемости узлов в других сетях. Так как UDP не требует установки соединений, отправленные пакеты будут просто теряться в полностью загруженных каналах связи. Атака на отказ в обслуживании являются общей угрозой для различных устройств и приложений. Они не специфичны для RIP. Соответственно, методы борьбы с ними также типичны – это использование средств обнаружения вторжений и анализ трафика, а еще те услуги по борьбе с низкоуровневым DDoS, которые предлагают крупные Internet провайдеры.

Ложные маршруты RIP. Протокол RIP для работы использует порт 520 и UDP. Маршрутизаторы слушают трафик на данном порту. Таким

образом, любой пакет соответствующего формата будет принят и обработан маршрутизатором. В случае если аутентификация RIP не используется или пароль пуст, злоумышленник сможет передать данному маршрутизатору неверные данные о маршрутах, перенаправив таким образом сетевой трафик через подконтрольные взломщику узлы. Первое, с чего злоумышленник должен начать свою атаку, это определить маршрутизаторы, использующие протокол RIP. Это можно сделать несколькими способами:

– можно прослушать трафик с помощью сниффера. Каждые 30 секунд маршрутизаторы обмениваются маршрутной информацией. Также обмен производится при изменении топологии;

– также злоумышленник может просканировать сеть на наличие узлов с открытым портом 520 UDP;

– наилучшим, а зачастую и единственным возможным решением является использование специализированного пакетного анализатора, позволяющего перехватывать и анализировать именно обновления таблиц маршрутов. Таким специализированным средством является утилита с незамысловатым названием ASS (Autonomous system scanner). Данная утилита позволяет осуществлять как активный, так и пассивный поиск маршрутизаторов и протоколов маршрутизации. В процессе сканирования ASS работает в активном режиме, по окончании переходит в пассивный, который только прослушивает трафик. Эта утилита поддерживает не только RIP, но и другие протоколы маршрутизации.

Понижение версии протокола RIP. При использовании протокола RIP версии 1 аутентификация не используется, и защита обеспечивается только посредством списков доступа. Обойти списки доступа можно с помощью подделки IP-адреса источника. Далее злоумышленнику необходимо заставить маршрутизатор использовать RIP версии 1. Сделать это можно с помощью генераторов пакетов, например такого, как nemesis.

Взлом хэша MD5. Для защиты протокол OSPF (Open Shortest Path First) использует MD5-аутентификацию. Соответственно, по аналогии со

взломом MD5 в протоколе RIP, здесь эту защиту также можно взломать. Атака на OSPF с помощью эксплоита OSPF Exploit. В маршрутизаторах Cisco с операционной системой IOS версий 11.2, 11.3 и 12.0 возможно переполнение буфера при получении большого числа OSPF HELLO-пакетов.

Слепые DoS-атаки на BGP-маршрутизаторы. Слепыми мы будем называть те атаки, которые не требуют каких-либо дополнительных знаний, кроме IP-адреса BGP (Border Gateway Protocol)-маршрутизатора. Простейшим сценарием такой DoS-атаки является SYN flood на порт TCP-179. Для реализации этой атаки на промышленный маршрутизатор необходимо использовать несколько десятков компьютеров, а лучше бот-сеть. Более интересным способом «затопления» целевого роутера BGP, использующего MD5-аутентификацию, является применение SYN TCP-пакетов с MD5-сигнатурами. Эта атака позволяет добавить вычислительную нагрузку на обработку MD5 атакуемым роутером.

Атака на BGP. Данные нарушения могут быть получены в результате осуществления следующих атак на протокол BGP. Протокол BGP работает на основе протокола TCP, прослушивая порт 179. Следовательно, протокол BGP уязвим для атак на TCP:

– **атака confidentiality violations** (нарушение конфиденциальности). Как уже упоминалось ранее, маршрутные данные BGP передаются в открытом текстовом виде, что позволяет легко перехватывать информацию (это происходит потому, что конфиденциальность маршрутных данных не является общим требованием);

– **атака replay** (воспроизведение). BGP не включает мер по предотвращению повторного использования перехваченных сообщений;

– **атака message insertion** (вставка сообщений). BGP не включает защиты от вставки сообщений. Однако, поскольку BGP использует транспортный протокол TCP, при завершенной организации соединения вставка сообщений внешним узлом потребует точного предсказывания

порядковых номеров (такое предсказание возможно, но весьма затруднено для хороших реализаций TCP) или перехвата сессий;

– **атака message deletion** (удаление сообщений). BGP не включает защиты от удаления сообщений. Опять-таки, такие атаки весьма затруднены для качественных реализаций TCP, но исключить их полностью нельзя;

– **атака message modification** (изменение сообщений). BGP не включает защиты от изменения сообщений. Синтаксически корректная модификация без изменения размера данных TCP в общем случае будет незаметной;

– **атака man-in-the-middle** (атаки с участием человека). BGP не включает защиты от MITM-атак. BGP не использует аутентификации партнером;

– **атака denial of service** (атаки на службы). Хотя ложные маршрутные данные сами по себе могут служит DoS-атакой на конечную систему, пытающуюся передавать данные через сеть, и сеть в целом, некоторые виды ложной информации могут создавать DoS-атаки на сам протокол BGP.

кибератаки на транспортном уровне (Transport layer) – на этом уровне используются два основных протокола TCP и UDP. Транспортный протокол (TCP) на сегодняшний день является наиболее распространенным средством транспортировки трафика. В отличие от протокола UDP, который может сразу же начать передачу пакетов, а TCP-соединение можно разделить на 3 стадии:

– установка соединения;

– передача данных;

– завершение соединения.

Сеанс протокола TCP может иметь одно из следующих состояний:

Closed – начальное состояние узла, фактически фиктивное;

Listen – сервер ожидает запросов установления соединения от клиента;

Syn-Sent – клиент отправил запрос серверу на установление соединения и ожидает ответа;

Syn-Received – сервер получил запрос на соединение, отправил ответный запрос и ожидает подтверждения;

Established – соединение установлено, идет передача данных;

Fin-Wait1 – одна из сторон (назовем ее узел1) завершает соединение, отправив сегмент с флагом FIN;

Close-Wait – другая сторона (узел2) переходит в это состояние, отправив, в свою очередь, сегмент ACK, и продолжает одностороннюю передачу;

Fin-Wait2 – узел1 получает ACK, продолжает чтение и ждет получения сегмента с флагом FIN;

Last-ACK – узел2 заканчивает передачу и отправляет сегмент с флагом FIN;

Time-Wait – узел1 получил сегмент с флагом FIN, отправил сегмент с флагом ACK и ждет 2*MSL секунд, перед окончательным закрытием соединения;

Closed – начальное состояние узла, фактически фиктивное.

Атака на TCP (IP-spoofing). Сегментом будем называть единицу данных протокола TCP, сессией – передачу данных в рамках одного соединения. Sequence number (последовательный номер) – это число, обозначающее номер первого байта в сегменте. Допустим, что некий пользователь «A» устанавливает TCP-соединение с пользователем «B», а злоумышленник пользователь «E» пытается вторгнуться в их «разговор», то есть осуществить атаку. Осуществление атаки происходит путем угадывания sequence number, B при установлении соединения между пользователями «A» и «B». На основе знаний о конкретной реализации TCP/IP можно предсказать, какой acknowledgement number будет выслан пользователем «B» на втором шаге установки соединения (рис.1.5).

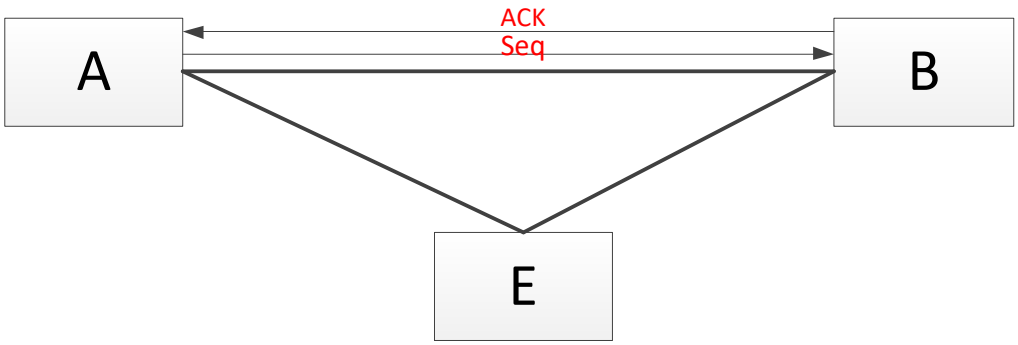

Рисунок 1.5 – Схема сетевого взаимодействия

Далее пользователю «E» необходимо ввести систему «B» в такое состояние, в котором она не сможет отвечать на сетевые запросы. Сделать это можно несколькими способами, например, дождаться перезагрузки системы данного пользователя. Затем злоумышленник «E» попытается притвориться пользователем «B», для того чтобы получить доступ к системе пользователя «A». Главное, что нужно сделать, для того чтобы «A» считал, что злоумышленник «E» – это добропорядочный пользователь «B» – отправить его системе сегмент от имени «B» с правильным acknowledgement number. Для этого «E» может отправить пользователю «A» несколько сегментов, инициирующих соединение, с целью выяснения sequence number. Анализируя ответы пользователя «A», взломщик «E» может предсказать, какой sequence number будет указан в следующем сегменте от «A». Поскольку ключевой элемент атаки – угадывание sequence number, то в защите от IP-spoofing может помочь использование криптографически стойкого алгоритма генерации псевдослучайных чисел для генерации sequence number.

TCP hijacking. Главная задача злоумышленника – привести соединение своих жертв в так называемое десинхронизованное состояние, то есть такое состояние, при котором соединение считается установленным, но acknowledgement number не совпадает с ожидаемым значением одной из сторон. Защититься от такой атаки можно, контролируя переход в десинхронизованное состояние, обмениваясь информацией о sequence

number, acknowledgement number. Но злоумышленник может менять эти значения, ведь он прослушивает пакеты. Более надежной защитой кажется леживание ACK-бурь.

Сканирование сети. Цель этой атаки в том, чтобы выяснить, какие компьютеры подключены к сети и какие сетевые сервисы на них запущены. Первая задача в простейшем случае решается путем посылки Echo-сообщений протокола ICMP (Internet Control Message Protocol) с помощью утилиты ping с последовательным перебором всех адресов сети или отправкой Echo-сообщения по широковещательному адресу. Анализируя трафик и леживая Echo-сообщения, посылаемые за короткий промежуток времени всем узлам, можно выявить попытки сканирования. Чтобы не дать себя раскрыть, злоумышленник может растянуть отправку сообщений во времени. Вместо Echo-сообщений могут применяться TCP-сегменты code bit RST, ответы на несуществующие DNS-запросы. Если злоумышленник получит в ответ ICMP Destination Unreachable пакет с кодом (host Unreachable), то, значит, тестируемый узел выключен или не подключен к сети. Чтобы определить, какие сервисы запущены, нужно узнать, какие порты открыты, так как существует набор сервисов, за которыми закреплены определенные порты. Далее эту информацию можно использовать для осуществления атаки на более высоком уровне. Для сканирования TCP-портов существует несколько способов. Самый простой – установление TCP-соединений с тестируемым портом. В этом случае появляется большое количество открытых и сразу прерванных соединений, поэтому атаку в такой реализации просто обнаружить. Другой способ – так называемый half-open scanning (сканирование в режиме половинного открытия). В этом режиме злоумышленник отправляет сегмент code bit RST, то это значит, что порт закрыт, а если сегмент с code bit RST, то это значит, что порт закрыт, а если сегмент code bit RST SYN, ACK – порт открыт. Тогда злоумышленник отправит на этот порт сегмент с флагом RST. Так как соединение не было открыто, то обнаружить это сканирование гораздо сложнее.

SYN flood. Атака состоит в отправке большого числа сегментов с флагом SYN. Это число больше, чем атакуемый узел, может обработать одновременно. Цель – привести узел в состояние, когда он не сможет принимать запросы на открытие новых соединений, а в худшем случае «зависнет». От имени несуществующего отправителя злоумышленник посылает TCP-сегмент с флагом SYN. Атакуемый узел, получив сегмент, отвечает сегментом с флагами SYN, ACK и переводит сессию в состояние SYN_Received. Если поступает сегмент-подтверждение, то есть сегмент с флагом ACK и нужным acknowledgement number, то соединение переходит в состояние Established, если подтверждения не поступает, то соединение удаляется из очереди. Когда очередь соединений уже заполнена, а система получает новый запрос на установление соединения, то этот запрос игнорируется. Если скорость и количество поступающих на маршрутизатор SYN-сегментов увеличиваются, то он переходит в такой режим работы, при котором время ожидания ответа от отправителя SYN-сегмента резко уменьшается, и вновь прибывший SYN-сегмент «выталкивает» из очереди ранее полученный. В этом случае советуют использовать программное обеспечение, которое позволяет установить максимальное число открываемых соединений и список разрешенных клиентов.

Атаки на UDP. Протокол дейтаграмм пользователя (User Datagram Protocol) предназначается для передачи данных между прикладными процессами и обменом дейтаграммами между компьютерами, входящими в единую сеть. Длина пакета в UDP измеряется в октетах, дейтаграммы пользователя включают заголовок и данные. Это означает, что минимальная величина длины – четыре байта. Протокол UDP является транспортным и не устанавливает логического соединения, а также не упорядочивает пакетов данных. То есть пакеты могут прийти не в том порядке, в котором они были отправлены, и UDP не обеспечивает достоверности доставки пакетов. Но данные, отправляемые через модуль UDP, достигают места назначения как единое целое. Главная особенность UDP заключается в том, что он сохраняет

границы сообщений и никогда не объединяет несколько сообщений в одно. На протокол UDP существует не так много атак, так на TCP. Это можно объяснить, прежде всего, тем, что этот протокол менее распространен. К тому же утствие установки соединения лишает самой возможности реализации целого ряда атак, характерных для TCP.

UDP Storm. Для осуществления данной атаки необходимо, чтобы на сервере было открыто как минимум два порта. Например, отправляется на один из открытых портов UDP-запрос, а в качестве отправителя указывается адрес второго открытого UDP-порта, и тут происходит самое интересное – порты отвечают друг другу бесконечно. В результате данной атаки снижается производительность сервера. Реализовать ее можно с помощью утилиты Nemesis. Многие системы телефонной связи через Internet (IP-телефония) организуют соединения на уровне инкапсулируемых в дейтаграммы UDP-данных (например, телефонное соединение между абонентами). Для таких приложений поток информации о недоступности удаленной стороны может приводить к разрыву соединения на уровне инкапсулированного в UDP протокола. UDP Package – смысл атаки заключается в отправке некорректного пакета на сервис UDP. Например, UDP-пакет с некорректными полями служебных данных. Попробовать реализовать данную атаку можно с помощью конструктора пакетов PackETH. Для протокола UDP так же, как и для других протоколов, характерны DoS-атаки «отказ в обслуживании». Для реализации данного вида атак необходимо сгенерировать большое количество UDP-пакетов, направленных на определенную машину. В результате успешной атаки происходит либо зависание, либо его перезагрузка. Осуществить атаку можно из-за того, что в UDP утствует механизм предотвращения перегрузок.

кибератаки на уровнях приложения (Session, Presentation and Application layers) – выше представлены кибератаки на протоколы четырех нижних уровней, а из верхних уровней (Session, Presentation and Application layers) кибератакам в большей степени подвергаются протоколы прикладного

уровня (Application layer). Собственно, различных протоколов, работающих на прикладном уровне, превеликое множество, так же как и количество различных сетевых приложений и сетевых систем. Начнем с протоколов, предназначенных для задач мониторинга – SNMP и Syslog.

Протокол SNMP. Изначально протокол SNMP разрабатывался для проверки функционирования сетевых маршрутизаторов. Впоследствии сфера действия протокола охватила и другие сетевые устройства, такие как концентраторы, шлюзы, терминальные серверы, машины под управлением Windows Server и т.д. Кроме того, протокол допускает возможность внесения изменений в функционирование указанных устройств. Основными участниками процесса функционирования протокола являются агенты и системы управления. Если рассматривать эти два понятия на языке «клиент-сервер», то роль сервера выполняют агенты, то есть те самые устройства, для опроса состояния которых и был разработан этот протокол. Протокол позволяет опрашивать устройства по сети, получая сведения о состоянии их сетевых интерфейсов, нагрузке и других данных. Также протокол SNMP обладает еще одной весьма важной особенностью, а именно возможностью модифицировать данные на агентах. Вся информация об объектах системы-агента содержится в так называемой MIB (management information base) – базе управляющей информации, другими словами, MIB представляет собой совокупность объектов, доступных для операций записи-чтения для каждого конкретного клиента, в зависимости от структуры и предназначения самого клиента. На данный момент существуют четыре базы MIB:

– **Internet MIB** – база данных объектов для обеспечения диагностики ошибок и конфигураций. Включает в себя более 200 объектов (в том числе и объекты MIB-I);

– **LAN manager MIB** – база из более 100 объектов – пароли, сессии, пользователи, общие ресурсы;

– **WINS MIB** – база объектов, необходимых для функционирования WINS-сервера (WINSMIB.DLL);

– **DHCP MIB** – база объектов, необходимых для функционирования DHCP-сервера (DHCPMIB.DLL), служащего для динамического выделения IP-адресов в сети.

SNMP – в целом протокол контроля и диагностики, в связи с чем он рассчитан на ситуации, когда нарушается целостность маршрутов, кроме того, в такой ситуации требуется как можно менее требовательный в аппаратуре транспортный протокол, потому выбор был сделан в сторону UDP. Таким образом, при использовании протокола SNMP необходимо быть предельно аккуратным. Для обеспечения безопасности устройств, мониторинг ведется через SNMP, необходимо использовать межсетевые экраны для сегментации и разрешения взаимодействия по данному протоколу только доверенных хостов. Для обнаружения устройств, поддерживающих SNMP, можно воспользоваться утилитой SNMP, входящей в состав дистрибутива Kali.

Протокол Syslog. Архивирование (журналирование) событий, происходящих в операционной системе, на устройстве или приложении, является неотъемлемой частью процесса обеспечения информационной безопасности. По наличию событий в журналах безопасности можно заблаговременно обнаружить попытку осуществления атаки на сеть. А в случае если инцидент все же произошел, записи в журнале могут помочь в его расследовании. Поэтому протокол прикладного уровня Syslog должен работать без сбоев.

В крупных сетях, как правило, для сбора событий используется центральный сервер Syslog, получающий события со всех устройств и приложений сети. Хакер пытается вскрыть конкретное устройство. В случае успеха он сможет почистить журнал событий на данном устройстве. Однако записи об этих событиях будут также сохранены на центральном сервере Syslog. Злоумышленнику останется только разработать сценарий, который будет в цикле отправлять сообщения. То есть если в сети не ведется сбор событий с пользовательских рабочих станций, то не сервере Syslog не

должны собираться события из пользовательского сегмента. Ограничить передачу событий можно средствами сетевого оборудования, запретив пересылку UDP-пакетов по 514-му порту.

Атака на DNS. Служба DNS является одним из самых критичных компонентов сети Internet, так как обеспечивает разрешение доменных имен сайтов. В случае отказа DNS доступ к ресурсам Interneta станет практически невозможен. Кроме того, в случае подмены сайта посредством изменения записей DNS пользователи попадут на поддельный сайт, или же трафик пойдет через маршрутизаторы, контролируемые злоумышленником. В частности, перенаправив запросы пользователей к службе Windows Update на поддельный сервер, хакеры могут добиться загрузки на пользовательские ПК вредоносных программ под видом обычных обновлений.

Атака на web-приложения через систему управления сессиями. Еще одним уязвимым местом являются web-приложения. Конечно, разработка корпоративных web-порталов обычно поручается профессионалам web-программистам, но системный администратор и тем более специалист по информационной безопасности должны иметь представление о существующих уязвимостях в web-приложениях. Кроме того, в небольших компаниях системный администратор зачастую занимается разработкой и поддержкой корпоративного портала.

Современные web-порталы используют в качестве web-сервера преимущественно Apache. Существует, конечно, IIS (Internet Information Services), работающий под Windows, но большинство хостингов все равно использует связку Free BSD/Linux+Apache. Для хранения данных, с которыми работает web-портал, обычно используется MySQL или Postgree SQL. В высоконагруженных промышленных системах может применяться Oracle. В качестве примера рассмотрим атаки на PHP-приложение через систему управления сессиями. Основными причинами возможности данных атак являются утствие проверки идентификатора сессии пользователя и утствие проверки данных, хранящихся в сессии.

Суть атаки (Session Hijacking) заключается в использовании злоумышленником идентификатора сессии, принадлежащего легальному пользователю, для выдачи себя за владельца сессии. Узнать идентификатор чужой сессии можно с помощью перехвата трафика легального пользователя, организации XSS-атаки или с помощью перебора. Общий алгоритм осуществления атаки следующий:

– атакующий собирает информацию об IP-адресах жертвы и том ресурсе, доступ к которому необходимо получить;

– затем необходимо дождаться, когда атакуемый подключится к целевому ресурсу;

– далее злоумышленнику необходимо запустить ARP relay;

– когда жертва подключилась к целевому ресурсу, а начала работу с ним, атакующий увидел в снифферe новое активное соединение. Далее взломщик производит атаку десинхронизацией TCP/IP, которая уже описывалась ранее;

– далее злоумышленник может работать от имени жертвы и с ее учетными правами;

– атакуемый вынужден заново переподключиться к целевому ресурсу, справедливо полагая, что произошел аппаратный сбой соединения. Злоумышленник отправляет ему RST;

– когда хакер закончит работу с системой, он прекращает посылать RST и отключает ARP-relay. Угроза отправленной сессии возникает, если злоумышленник имеет возможность установить свой PHP-сценарий на сервере, где исполняется атакуемое приложение. Отправление возможно, если атакуемое приложение имеет ошибку, позволяющую выполнять произвольный код, и если web-приложение работает на сервере вместе с приложениями других пользователей хостинга.

Среди рассмотренных выше кибератак наиболее сложной кибератакой на сегодняшний день является DDoS-атаки. **Ниже рассмотрим**

крупномасштабные DDoS-атаки на банковские информационные системы и сети крупных компаний мира [50, 51, 55, 56].

- **2007 г. Компьютерные сети Эстонии подверглись атаке.** Последствия: пострадала торговля – были проблемы с кассовым, платежным оборудованием, системы работали со сбоями. Злоумышленники практически вывели из строя электронные почтовые сервисы, каналы передачи информации были забиты спамом. Исчерпывающей информации о мощности атаки нет. Но поражает другое – время активности атакующих. Около 3 недель бети рассылали огромные объемы спама, заваливая эстонскую сеть запросами.
- **2012 г. – атаковали американские банки.** Мощность атаки: 60 Гбит/с. Последствия: под обстрел попали сразу 6 банков США: Bank of America, JP Morgan Chase, US Bank, Citigroup, Wells Fargo и PNC Bank. Злоумышленники использовали разные способы, проверяя от какого типа атаки банки менее всего защищены.
- **2015 г. Сайт Центрального Банка РФ подвергся атаке.** В 2015 году каждый четвертый банк Российской Федерации (РФ) сталкивался с DDoS-атаками. По сравнению с 2014 годом, рост числа DDoS-атак на финансовые учреждения – 50%, на предприятия сектора электронной коммерции – 70%, туристической сферы – 150%. Самым атакуемым стал рынок недвижимости, здесь число DDoS-атак возросло на 170%.
- **2017 г. – атаковали Google.** Мощность атаки: 2,54 Тбит/с. Последствия: сервисы Google работали без сбоев, данные пользователи не пострадали. На данный момент это самая мощная DDoS-атака в истории. По данным Google Threat Analysis Group (TAG), источником атаки был Китай. Аналитики возложили ответственность за нее на «правительственных хакеров». Атака мощностью 2,54 Тбит/с стала кульминацией полугодичной кампании, которую хакеры вели против Google. В течение 6 месяцев злоумышленники использовали разные методы в попытках подорвать работу инфраструктуры корпорации.

2018 г. – атаковали GitHub. Мощность атаки: 1,35 Тбит/с. Последствия: работа сервиса замедлилась примерно на 4 минуты, еще на 5 минут он был выведен из строя. Затем атакующие прекратили свои действия. Справиться с наплывом мусорного трафика GitHub помог CDN-провайдер Akamai. После атаки администраторы признали, что атакующие использовали дыры в безопасности самой площадки. Для генерирования трафика не понадобился объемный ботнет – достаточно было надавить на уязвимости Memcached-серверов.

2020 г. – атаковали клиента Amazon Web-Services. Мощность атаки: 2,3 Тбит/с. Последствия: специалисты AWS посчитали, что каждая минута простоя обходится бизнесу в 5600 долларов, однако эта цифра может меняться в зависимости от региона и направления деятельности компании. Атака длилась 3 дня. Однако клиенты AWS не столкнулись с масштабными сбоями в работе сервиса.

2021 г. – атаковали Яндекс. Мощность атаки: 21,8 млн. запросов/с. Последствия: несмотря на масштаб, атака не повлияла на работу сервисов Яндекса. Данные пользователей также не пострадали. Через несколько дней после атаки Яндекс опубликовал в блоге на Хабре некоторые результаты расследования, которое компания проводила совместно с коллегами из Qrator Labs. Из материала следует, что специалисты еще в июне 2021 года начали замечать признаки ботнета нового типа с несколькими сотнями тысяч устройств. Исследователи связывают его с крупнейшими атаками, которые в августе/сентябре 2021 года были зафиксированы в Новой Зеландии, США и России.

Также результаты анализа [6-17] показывают, что наиболее опасными для компьютерных сетей является компьютерная атака (КА) «отказ в обслуживании» (Denial of Service – DoS) и «распределенный отказ в обслуживании» (Distributed Denial of Service – DDoS). В атаке DoS, DDoS участвуют сотни или даже тысячи взломанных хостов, которые нападают на один целевой объект (сервер). Этими «зомби» – хостами неумышленно

становятся миллионы незащищенных компьютеров, которые выходят в Internet через широкополосные постоянно-активные соединения. Подсаживая на эти компьютеры «спящие» коды, хакеры получают возможность быстро создать целые легионы «зомби», которым достаточно лишь дать команду на запуск атаки DDoS. Если в атаке участвует достаточно большое количество «зомби» – хостов, ее масштабы могут быть поистине колоссальными.

Применение этого типа КА для нанесения ущерба объясняется простотой и малой стоимостью их организации, тем, что для их реализации нет необходимости в глубоких знаниях компьютерных технологий и языков программирования. Атаки DoS и DDoS часто встречаются в мире Internet безопасности. Во-первых, они не направлены на уязвимости, которые могут быть исправлены; во-вторых, каждый отдельный пакет является вполне легитимным – лишь их совокупность приводит к разрушительным последствиям, и, в-третьих, такие атаки носят продолжительный характер – они длятся несколько часов или дней, вместо нескольких секунд или минут.

Многие группы хакеров начали использовать DoS/DDoS – атаки, финансово мотивированные преступные организаций и даже правительственные структуры заинтересовались открывающимися возможностями. Первые подобные атаки против банков были отмечены в США во второй половине 2012 года. Через каналы Internet на банковские сайты иногда направлялось в секунду до 70 гигабит шумового трафика. До сих пор большинство атак на уровне сети поглощало не более пяти гигабит в секунду. Переход на уровень приложений и повышение интенсивности атак приводило к полной невозможности использования сайтов. Но основной задачей DDoS-атак, по мнению аналитиков, является отвлечение внимания служб безопасности банков. В отчете Gartner приводятся примеры того, как мошенники входят в доверие к клиентам банков, представляясь сотрудниками полиции или служащими банка, которым поручено помочь клиенту перейти на новый счет.

Принцип реализации типовой DDoS-атаки: DDoS-атака – это скоординированное действие, направленное на нарушение доступности услуг (сервисов) некоторой системы или сетевого ресурса, инициированное использованием множества скомпрометированных компьютеров (хостов), размещенных в сети Internet. Она базируется на использовании множества отдельных DoS-атак. Злоумышленник контролирует один или несколько северов, на которых размещаются агенты-мастера. При атаке тысячи компьютеров обращаются с запросами к серверу, заставляя его реагировать на них. Огромное количество компьютеров заражено вирусами и троянами, и злоумышленник может послать управляющую команду этим узлам. Такие компьютеры называются «зомби». Это именно из них и сформирована «беть», то есть сеть зараженных узлов, которой управляет злоумышленник. В результате вся эта сеть начнет обращаться с запросами к целевой системе (сервер). Пытаясь обработать все запросы, она просто не будет иметь возможности отвечать легитимным пользователем. Цель злоумышленника достигнута. DDoS-атаки считается успешным, если в результате информационной ресурс становится недоступен (рис.1.6).

Рисунок 1.6 – Принцип реализации типовой DDoS-атаки

Последствия атаки типа «DDoS»: атакуемый сервер исчерпывает свои аппаратные ресурсы и лимиты запросов. В зависимости от типа конкретной DDoS-атаки, это может быть:

– пропускная способность канала связи;

– лимит на количество устанавливаемых соединений;

– физическая память сервера;

– количество процессов web-сервера;

– перегрузка дисковой подсистемы и базы данных.

Web-сайты под DDoS-атакой сначала открывается медленно, затем может вообще не открываться с ошибкой 500 в браузере или просто с ошибкой о невозможности установки соединения. DDoS-атака на IP-адрес характеризуется тем, что все сайты и Internet-сервисы на данном сервере прекращают нормально работать. Возможна полная потеря соединения с сервером по протоколу SSH или FTP. Нарушаются обязательства по договорам обслуживания (Service-level agreements, SLA) и приходится возвращать немалые деньги за неоказанные услуги. На репутацию банков (или компаний) ложится темное пятно. Неполученные прибыли, падение производительности, рост расходов на ИТ, судебные издержки – убытки ширятся и растут.

Основные виды атаки типа «DDoS»:

UDP flood – отправка на адрес системы-мишени множества пакетов UDP (User Datagram Protocol);

TCP flood – отправка на адрес мишени множества TCP-пакетов, что также приводит к «связыванию» сетевых ресурсов;

TCP SYN flood – посылка большого количества запросов на инициализацию TCP-соединений с узлом-мишенью, которому в результате приходится расходовать все свои ресурсы на что, чтобы леживать эти частично открытые соединения;

Smurf-атака пинг-запросы ICMP (Internet Control Message Protocol) по адресу направленной широковещательной рассылки с использованием в

пакетах фальшивого адреса источника. Таким образом, создается большой объем данных, которые будут посланы в ответ;

ICMP flood – атака, аналогичная Smurf, но без использования рассылки. Самое большое распространение получила DDoS-атака с использованием TCP SYN flood, поскольку в данном случае атакующим всего один пакет на открытие соединения. Такие атаки не нуждаются в обратной связи с атакующим, и поэтому можно не использовать настоящий адрес источника. Потому в отличие от остальных видов атак нет возможности построить список «плохих» IP-адресов, с которых производится атака.

Поскольку DDoS относятся к тем атакам, защититься от которых труднее всего, перед всеми компаниями, которые зависят от сети Internet, стоит сложная задача – применять против этих атак действенные и эффективные меры. Сетевые элементы (устройства) и традиционные технологии периметрической защиты, в частности, межсетевые экраны и системы выявления вторжений (IDS), хотя и служат важными составляющими стратегии безопасности в целом, не обеспечивают полномасштабную защиту от DDoS. Для защиты от современных DDoS-атак, направленных на нарушение работы банковских услуг, требуется специально разработанная архитектура, в которой, в частности, должна быть способна обнаруживать и нейтрализовать все более сложные, изощренные и неуязвимые атаки.

Но в любом случае для защиты от DDoS-атак требуется высокоскоростной канал доступа к Internet, желательно дублированный. Одним из решений для защиты от атак может служить приобретение автономной системы БИС. Это системы IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с Internet. Таким образом, приобретая БИС, мы получаем свой собственный сегмент сети, который не зависит от остальной

части Internet. Каждая система имеет информационные каналы с другими системами, которые входят в состав базовой сети Internet.

Пакеты инструментов для DDoS-атак: Пакеты инструментов, для использования которых не требуется писать код или быть опытным хакером, позволяют новичкам легко настроить беть. Пакет инструментов для DDoS-атак представляют собой пакет программного обеспечения (ПО), состоящего из компонентов – конструктора ботов и сервера управления:

Bot Builder – инструмент для пошагового создания ботов с графическим интерфейсом, который позволяет атакующему создать исполняемый файл (бот), распространяемый на компьютеры, которые будут являться частью бети;

Центр управления (Command Control, C&C) – представляет собой страницу администратора, которая используется злоумышленником для леживания состояния ботов и отправления команд. Основные причины организации DDoS-атаки представлены на рисунке 1.7 [15-20]:

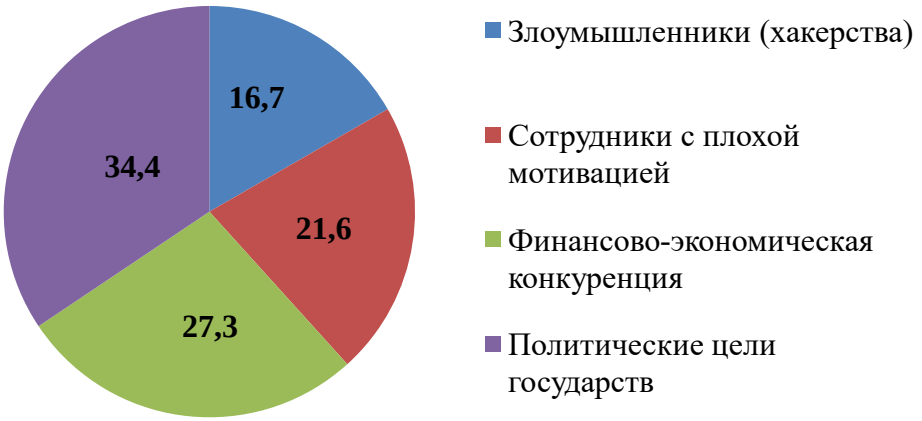

Рисунок 1.7 – Основные причины DDoS-атак, %

В таблице 1.4 приведена классификация используемых технологий, целей и последствий КА «DDoS» по модели ISO/OSI.

Таблица 1.4 – Классификация используемых технологий, целей и последствий DDoS-атаки по модели ISO/OSI

№	Уровни ISO/OSI	Тип данных	Описание уровня	Протоколы	Примеры технологий DDoS (DoS)	Последствия DDoS-атаки
1	Физический	Биты	Передача двоичных данных	100BaseT, 1000 Base-X	Физическое разрушение, физическое препятствие работе или управлению физическими сетевыми активами	Сетевое оборудование приходит в негодность и требует ремонта для возобновления работы
2	Канальный	Кадры	Установка и сопровождение передачи сообщений на физическом уровне	G.802.3, G.802.5	MAC-flood переполнение пакетами данных сетевых коммутаторов	Потоки данных от отправителя получателю блокируют работу всех портов
3	Сетевой	Пакеты	Маршрутизация и передача информации между различными сетями	IP, ICMP, ARP, RIP	ICMP- flood, используют ICMP-сообщения для перегрузки пропускной способности целевой сети	Снижение пропускной способности атакуемой сети и возможная перегруженность брандмауэра
4	Транспортный	Сегменты	Обеспечение безошибочной передачи информации между узлами, управление	TCP, UDP	SYN flood, Smurf-c запросами ICMP-сообщения	Достижение пределов по ширине канала или по количеству допустимых подключений, нарушение работы

			передачей сообщений с 1 по 3 уровни			сетевого оборудования
5	Сеансовый	Данные	Управление установкой и завершением соединения, синхронизацией сеансов в рамках операционной системы через сеть	RPC, PAP	Атака на протокол Telnet использует слабые места программного обеспечения Telnet-сервера на switch, делая сервер недоступным	Делает невозможным для администратора управление switch
6	Представительский	Данные	Трансляция данных от источника получателю	ASCII, EBCDIC	Подложные SSL запросы, проверка шифрованных SSL пакетов очень ресурсоемка, злоумышленники используют SSL для HTTP-атак на сервер жертвы	Атакуемые системы могут перестать принимать SSL соединения или автоматически перегружаться
7	Прикладной	Данные	Начало создания пакетов данных.	FTP, HTTP, POP3, SMTP	PDFGET запросы HTTPGET, HTTPPOST (формы веб-сайтов, логин, подтверждение обратной связи)	Нехватка ресурсов. Чрезмерное потребление системных ресурсов службами на атакуемом сервере

ГЛАВА 2. МАТЕМАТИЧЕСКИЕ МОДЕЛИРОВАНИЯ ПРОЦЕССОВ КИБЕРАТАК НА БАНКОВСКИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

2.1. Краткий обзор методов моделирования процессов кибератак на БИС. В настоящее время для анализа и синтеза сложных организационно-технических систем разработаны достаточно универсальные методы, ориентированные на различные предметные области и свойства систем. При исследовании оперативности (своевременности) систем управления связью наиболее широкое распространение получили графо-аналитический, логико-вероятностный, метод Марковских цепей и метод топологического преобразования стохастических сетей. Сходство методов состоит в том, что они используют как структурную, так и неструктурную информацию об исследуемых объектах, имеющих, как правило, вероятностную (случайную) природу. Структура при этом задается в виде различных графов, а неструктурная информация определяется весовыми коэффициентами, задаваемыми на вершинах и ребрах графа. Весовые коэффициенты могут быть и вероятностными, и детерминированными [6-13].

Графо-аналитический метод предполагает исследование процессов обмена сообщениями по сети связи, структура которой может изменяться при различных внутренних и внешних воздействиях и управляющих воздействиях системы управления сетью связи. В графо-аналитических моделях структуры представлены физически наиболее наглядно, а вероятностные или детерминированные весовые коэффициенты являются однородными. При применении указанного метода сеть связи представляется вероятностным или детерминированным взвешенным графом, вершинам которого ставятся в соответствие узлы связи, а ребрам – каналы связи, их соединяющие. При этом весовыми коэффициентами являются значения вероятностных или детерминированных величин, характеризующих различные свойства узлов и каналов связи, эффективность протоколов управления на различных уровнях. Задачи анализа сети сводятся к поиску

путей между произвольными вершинами, отбору множества путей, удовлетворяющих заданным требованиям, производству операций сложения, умножения или взятия минимума и получению результата, зависящего от структуры сети и характеристик ее компонентов. Метод широко применяется в мировой практике для исследования сетей общего пользования. Однако для применения его к исследованию систем технологического назначения, таких как БИС, требуется разработка достаточно сложных моделей для определения весовых коэффициентов, учитывающих специфику их функционирования [6-13].

В логико-вероятностном методе структура исследуемой системы представляется логической схемой функциональной целостности, отражающей логику взаимодействия элементов системы, при которой сохраняется ее работоспособность. Аппаратом для описания схемы функциональной целостности является алгебра логики. При этом неструктурная информация представляется значениями вероятностей свершения событий, входящих в схему функциональной целостности. На основе схемы функциональной целостности и вероятностей событий получают многочлен, используемый для определения вероятности свершения (или не свершения) сложного события, составленного из множества элементарных событий, логика взаимодействия которых определяется схемой функциональной целостности. Данный метод хорошо работает при оценке надежности систем в случае, когда точность определения вероятностей событий достаточно велика и основана на больших статистических выборках. Метод позволяет определять вклад и значимость отдельных элементов, выявляя наиболее проблемные места, влияющие на надежность и, соответственно, на безопасность работы сложной системы. В случае применения указанного метода для исследования динамичных конфликтных вероятностных процессов в условиях значительной неопределенности возникают сложности, связанные с получением непрерывной временной картины по отдельным фрагментам – временным

сечениям, для которых составляется схема функциональной целостности. Кроме того, возникают трудности добывания исходных данных для определения вероятностей многочисленных событий, что связанно с присущей конфликтным ситуациям неопределенностью [6-13].

Для исследования процессов управления и связи, также широко применяются **дискретные цепи Маркова А.А.** Такой метод позволяет учитывать действия злоумышленника, состояние влияющей на сеть связи среды, способы организации управления и связи. При этом структура системы задается графом состояний, вершинам которого соответствуют возможные состояния, а ребрам – направления возможных переходов из одного состояния в другое. В качестве весовых коэффициентов используются вероятности состояний – начальное и через *n* шагов. Начальное состояние задается распределением вероятностей состояний, а состояние системы на *n* – м шаге является решением Марковской цепи. Весовыми коэффициентами ребер являются вероятности перехода из одного состояния в другое за один шаг. При применении метода дискретных Марковских цепей необходимо определить, что является состоянием системы, каковы возможные состояния системы, что является шагом и в какие моменты времени производятся шаги, а также какие переходы из одного состояния в другое возможны за один шаг. В результате применения метода дискретных Марковских цепей к исследованию процессов управления связью могут быть обоснованы способы рациональной организации управления связью в заданных условиях. Сложности применения метода заключаются в получении исходных данных, а также в доказательстве соответствия исследуемого процесса дискретному Марковскому [6-13, 31, 48].

Метод топологического преобразования стохастических сетей (ТПСС) является более абстрактным, чем рассмотренные выше. Поэтому он применим к исследованию более широкого класса случайных процессов, происходящих в сложных организационно-технических системах, таких как БИС [6-13, 31, 48].

Суть метода заключается в том, что исследуется не система, а реализуемый ей целевой процесс. Этот сложный процесс декомпозируется на элементарные процессы, каждый из которых характеризуется функцией распределения времени выполнения процесса, плотностью вероятности, вероятностью или средним и дисперсией времени выполнения. Логика и последовательность выполнения процессов определяется двухполюсной сетью, состоящей из входного, промежуточных и выходного узлов (вершин) – стохастической сетью. Под стохастической сетью можно понимать совокупность взаимоувязанных узлов (вершин) и ветвей, соединение которых соответствует алгоритму функционирования исследуемой системы. При этом сеть реализуется, если будет выполнено некоторое подмножество ветвей, время реализации которых выбирается в соответствии с вероятностным распределением. Ребрам сети соответствует набор элементарных процессов, а узлам – условия их выполнения. Каждый узел выполняет две функции – входную, определяющую условие выполнения узла, и выходную, определяющую, какие из операций, следующих за узлом будут выполняться. Входной узел сети выполняет только выходную функцию, а выходной – только входную. Для каждого из ребер определяется функция передачи – условная характеристическая функция, являющаяся преобразованием Лапласа плотности распределения вероятностей времени выполнения элементарной операции (процесса). Затем выполняется топологическое преобразование сети случайных процессов. Известно, что топология является разделом математики, в котором изучаются свойства геометрических фигур, не изменяющиеся при любых деформациях, производимых без разрывов и склеиваний. Главной задачей топологии является изучение таких топологических свойств как связность, компактность, размерность и др. В данном случае таким топологическим инвариантом является свойство связности графа. Поскольку входная и выходная вершины двухполюсной сети (графа) являются связными, то с помощью стандартных процедур ее можно свести к одному ребру,

связывающему эти вершины. Для этого в сети сначала выделяются последовательные, параллельные и петлеобразные пути, на которых определяются эквивалентные функции передачи и каждый из которых сводится к одному ребру. Затем с помощью правила Мейсона эти фрагменты объединяются также в одно ребро с общей эквивалентной функцией передачи. При этом структура сети не исчезает бесследно – ее «следы» остаются в структуре эквивалентной функции. После получения эквивалентной функции производят обратное преобразование Лапласа, результатом которого является функция плотности распределения вероятностей времени выполнения целевого процесса, либо определяют начальные моменты случайного времени его выполнения. Таким образом, сущность метода ТПСС состоит в представлении анализируемого процесса в виде стохастической сети, замене множества элементарных ветвей сети одной эквивалентной и последующим определением эквивалентной функции сети, начальных моментов и функции распределения случайного времени ее реализации, т.е. реализации анализируемого процесса. Из сущности метода ТПСС следует, что для его применения необходимо правильное, не искажающее физического смысла представление анализируемого процесса функционирования системы связи или ее элемента стохастической сетью. К достоинствам метода относится возможность представления процессов с различной степенью глубины детализации набором вложенных моделей. С одной стороны, это позволяет точнее получать исходные данные для моделей более высокого уровня, а с другой – определять необходимый уровень детализации. Также метод отличается ясным физическим смыслом при постановке задачи и высокой степенью формализации остальных этапов – топологического преобразования сети, получения эквивалентной функции и обратного преобразования Лапласа, что позволяет контролировать адекватность модели физическому процессу на всех этапах ее реализации [6-13, 31, 48].

Для моделирования процессов кибератак на элементы БИС применялся именно метод ТПСС. Его выбор был обусловлен еще и тем, что исходные данные о кибератаках на элементы банковских информационных систем доступны только на уровне их средних значений, а существующее регламентное описание самого процесса кибератак неоднозначно и достаточно сложно. Однако представляется возможным разделить искомый процесс на ряд более тривиальных подпроцессов, учитывая вероятностно-временные характеристики каждого из них в отдельности. В результате моделирования определяются функции распределения времени реализации отдельных подпроцессов, на основе которых строится комплексная модель процесса функционирования банковских информационных систем.

2.2. Частные модели кибератак на элементы БИС. Анализ работы показывают [6-22], что элементы банковских информационных систем в большой степени подвергаются следующим видам кибератак – «Логическое отключение абонентов», «Сканирование сети и ее уязвимостей» и DDoS-атаки.

Профильная модель компьютерной атаки типа «Логическое отключение абонентов».

Постановка задачи – задана банковская информационная система (БИС) состоящая из n элементов (маршрутизаторы, коммутаторы, серверы и мультифункциональные абонентские терминалы). Злоумышленник (хакер) совершает компьютерную атаку «Логическое отключение абонентов» в следующий запуск программно-аппаратного комплекса (сетевого сканера) за среднее время $\bar{t}_{вкл}$ с функцией распределения времени $W(t)$. Перехват IP-адресов абонентов атакуемой БИС с вероятностью P_n за среднее время $\bar{t}_{перех}$ с функцией распределения времени $Q(t)$. Изменение IP-адресов абонентов атакуемой БИС с вероятностью P_n за среднее время $\bar{t}_{изм}$ с функцией распределения времени $D(t)$. Отключение абонентов за среднее время $\bar{t}_{откл}$ с

функцией распределения $O(t)$. При этом, если IP-адрес не перехвачен, то с вероятностью $(1-P_n)$ выполняется их повторный перехват за среднее время $\bar{t}_{повт}$ и функцией распределения времени $Z(t)$.

Решение:

Описанный в постановке задачи процесс реализации «Логическое отключение абонентов» на сетевые элементы БИС представим в виде стохастической сети, приведенной на рисунке 2.1.

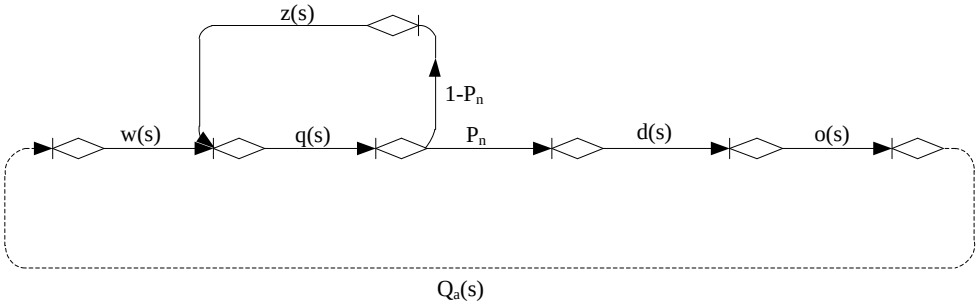

Рисунок 2.1 – Стохастическая сеть процесса реализации кибератаки «Логическое отключение абонентов» на сетевые элементы БИС

Нам заданы функции распределения и время реализации каждого процесса атаки злоумышленника: $w=\frac{1}{\bar{t}_{вкл}}$; $q=\frac{1}{\bar{t}_{перех}}$; $d=\frac{1}{\bar{t}_{изм}}$; $o=\frac{1}{\bar{t}_{откл}}$; $z=\frac{1}{\bar{t}_{повт}}$.

Время реализации данных процессов характеризуются экспоненциальным законом распределения:

$W(t)=1-e^{-w\cdot t}$; $Q(t)=1-e^{-q\cdot t}$; $D(t)=1-e^{-d\cdot t}$; $O(t)=1-e^{-o\cdot t}$; $Z(t)=1-e^{-z\cdot t}$.

В стохастической сети обозначено (рис.2.1): $w(s)$, $q(s)$, $d(s)$, $o(s)$ и $z(s)$ – преобразования Лапласа-Стилтьеса соответствующих функций распределения, указанных в постановке задачи и определяемых как (2.1):

$$r_i(s)=\int_0^{\infty}\exp(-st)d[R_i(t)]=\frac{r_i}{r_i+s} \qquad (2.1)$$

С целью определения эквивалентной функции стохастической сети (рис.2.1) замкнем вход и выход стохастической сети фиктивной ветвью

$Q_a(s) = \frac{1}{Q(s)}$ и перечислим петли первого и второго порядков [6-13, 31, 48]. С использованием уравнения Мейсона $H = 1 + \sum_{i=1}^{k} (-1)^k \cdot Q_k(s) = 0$, где $Q_k(s)$ - эквивалентные функции петель k-го порядка, определим эквивалентную функцию стохастической сети (2.2):

$$Q(s) = \frac{w(s) \cdot q(s) \cdot P_n \cdot d(s) \cdot o(s)}{1 - z(s) \cdot q(s) \cdot (1 - P_n)} \tag{2.2}$$

Подставим уравнения соответствующих функций распределения в функцию (2.2) и получим конечное уравнение эквивалентной функции (2.3):

$$\begin{aligned} Q(s) &= \frac{\frac{w}{w+s} \cdot \frac{q}{q+s} \cdot \frac{d}{d+s} \cdot \frac{o}{o+s} \cdot P_n}{1 - \frac{z}{z+s} \cdot \frac{q}{q+s} \cdot (1 - P_n)} = \\ &= \frac{w \cdot q \cdot d \cdot o \cdot P_n \cdot (z+s)}{\left[(z+s) \cdot (q+s) - z \cdot q \cdot (1 - P_n)\right] \cdot (w+s) \cdot (d+s) \cdot (o+s)} = \end{aligned} \tag{2.3}$$

Представим знаменатель уравнения (2.3) в форме:

$s^5 + A \cdot s^4 + B \cdot s^3 + C \cdot s^2 + D \cdot s + E$ по теореме Хэвисайда запишем эквивалентную функцию в виде (2.4):

$$h(s) = \sum_{i=1}^{5} \frac{w \cdot q \cdot P_n \cdot d \cdot o \cdot (z + s_i)}{\left[5 \cdot s_i^4 + 4 \cdot A \cdot s_i^3 + 3 \cdot B \cdot s_i^2 + 2 \cdot C \cdot s_i + D\right] \cdot (s - s_i)} \tag{2.4}$$

Тогда, используя обратное преобразование Лапласа для уравнения (2.4), получим функцию плотности распределения вероятностей времени (2.5):

$$h(t) = \sum_{i=1}^{5} \frac{\left[w \cdot q \cdot P_n \cdot d \cdot o \cdot (z + s_i)\right] \cdot e^{s_i \cdot t}}{\left[5 \cdot s_i^4 + 4 \cdot A \cdot s_i^3 + 3 \cdot B \cdot s_i^2 + 2 \cdot C \cdot s_i + D\right]} \tag{2.5}$$

После определения функции плотности вероятности времени $h(t) = L^{-1} \cdot \left[h(s)\right]$ можно определить функцию распределения методом обращения [31, 48]:

$$H(t)=\sum_{i=1}^{5}\frac{\left[w\cdot q\cdot P_n\cdot d\cdot o\cdot\left(z+s_i\right)\right]\cdot\left(1-e^{s_i\cdot t}\right)}{\left[5\cdot s_i^4+4\cdot A\cdot s_i^3+3\cdot B\cdot s_i^2+2\cdot C\cdot s_i+D\right]\cdot\left(-s_i\right)} \quad (2.6)$$

Расчет функции распределения методом двухмоментной аппроксимации и среднего времени реализации кибератаки. Так как (2.3), по определению, является характеристической функцией, то ее дифференцирование позволяет найти первый и второй начальные моменты случайного времени реализации моделируемого процесса, т.е. (2.7):

$$M_1(s,P_{\text{п}})=-\frac{d}{ds}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0},$$
$$M_2(s,P_{\text{п}})=\frac{d^2}{ds^2}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0} \quad (2.7)$$

юда среднее время реализации кибератаки равно (2.8):

$$\overline{t}_{\text{р}}(P_{\text{п}})=-\frac{d}{ds}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0} \quad (2.8)$$

Дисперсия времени реализации кибератаки «Логическое отключение абонентов» $D(\overline{t}_{\text{р}})$, определяемая как второй центральный момент, представлена выражением (2.9):

$$D(\overline{t}_{\text{р}})=\frac{d^2}{ds^2}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0}-\left\{-\frac{d}{ds}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0}\right\}^2 \quad (2.9)$$

Вычисление математического ожидания и дисперсии позволяет с достаточной для инженерных расчетов точностью определить интегральную функцию распределения времени успешной реализации кибератаки «Логическое отключение абонентов», как неполную Гамма-функцию (2.10):

$$F\left(t\right)=\begin{cases}0, \text{ если } t<0;\\ \int_0^t\frac{\mu^{\alpha}}{\Gamma(\alpha)}\cdot t^{\alpha-1}\cdot e^{-\mu\cdot t}dt, \text{ если } t>0\end{cases}, \quad (2.10)$$

где $\alpha=\frac{[\overline{t}_{\text{р}}(P_{\text{п}})]^2}{D(\overline{t}_{\text{р}})}$ - параметр формы; $\mu=\frac{\overline{t}_{\text{р}}(P_{\text{п}})}{D(\overline{t}_{\text{р}})}$ - параметр масштаба.

Результат: расчеты производились с использованием программного комплекса Mathcad-2014. По формуле (2.10) произведены расчеты, результаты которых представлены на рисунке 2.2. В качестве исходных данных использовались следующие значения среднего времени реализации частных процессов:

$\overline{t}_{вкл} = 2\,мин;$ – среднее время запуска программно-аппаратного комплекса (сетевого сканера);

$\overline{t}_{перех} = 5\,мин;$ – среднее время перехвата IP-адресов абонентов БИС;

$\overline{t}_{изм} = 6\,мин;$ – среднее время изменения IP-адресов абонентов БИС;

$\overline{t}_{откл} = 15\,мин;$ – среднее время отключение легитимных абонентов БИС;

$\overline{t}_{повт} = 14\,мин;$ – среднее время повторного запуска;

$P_n = 0,87$ – вероятность перехвата трафиков.

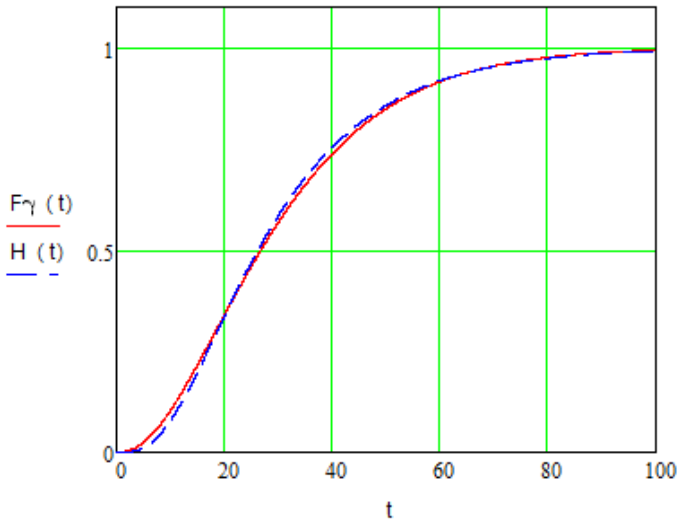

Рисунок 2.2 – Зависимость интегральной функции распределения вероятностей от времени реализации кибератаки «Логическое отключение абонентов» при успешной реализации с вероятностью P_n

Вывод: в ходе данной работы был смоделирован процесс компьютерной атаки типа «Логическое отключение абонентов». Для этого было произведено описание процесса атаки. На основе заданных исходных данных была построена стохастическая сеть обеспечивающая представление

анализируемого процесса. Для полученной стохастической сети была определена эквивалентная функция. Вероятностно-временные характеристики стохастической сети определились двумя различными методами (обращения и двухмоментной аппроксимации). При определении функции распределения методом обращения, мы получаем наиболее точную оценку процесса реализации компьютерной атаки. По полученным графикам, представленным на рисунке 2.2, видно, что функции, полученные двумя различными методами, совпадают.

Профильная модель компьютерной атаки типа «Сканирование сети и ее уязвимостей».

Постановка задачи – задана банковская информационная система (БИС) состоящая из n элементов (маршрутизаторы, коммутаторы, серверы и мультифункциональные абонентские терминалы). Злоумышленник совершает компьютерную атаку «Сканирование сети и ее уязвимостей» в следующей последовательности: запуск программно-аппаратного комплекса (сетевого сканера) за среднее время $\bar{t}_{зап}$ с функцией распределения времени $W(t)$. Определение активных элементов атакуемой БИС за среднее время $\bar{t}_{оп.элем}$ с функцией распределения времени $M(t)$, получается с вероятностью P_n. Определение типов операционных систем на активных элементах атакуемой БИС за среднее время $\bar{t}_{оп.ос}$ с функцией распределения времени $D(t)$. Определение сервисов на элементах атакуемой БИС за среднее время $\bar{t}_{оп.серв}$ с функцией распределения времени $L(t)$, получается с вероятностью P_n . Определение уязвимостей элементов атакуемой БИС за среднее время $\bar{t}_{оп.уязв}$ с функцией распределения времени $K(t)$. При этом, если активные элементы БИС, типы операционных систем и сервисы на них не будет определены, то с вероятностью $(1-P_n)$ сетевой сканер запускается повторно за среднее время $\bar{t}_{повт}$ с функцией распределения времени $Z(t)$.

Решение:

Описанный в постановке задачи процесс реализации «Сканирование сети и ее уязвимостей» на сетевые элементы БИС представим в виде стохастической сети, приведенной на рисунке 2.3.

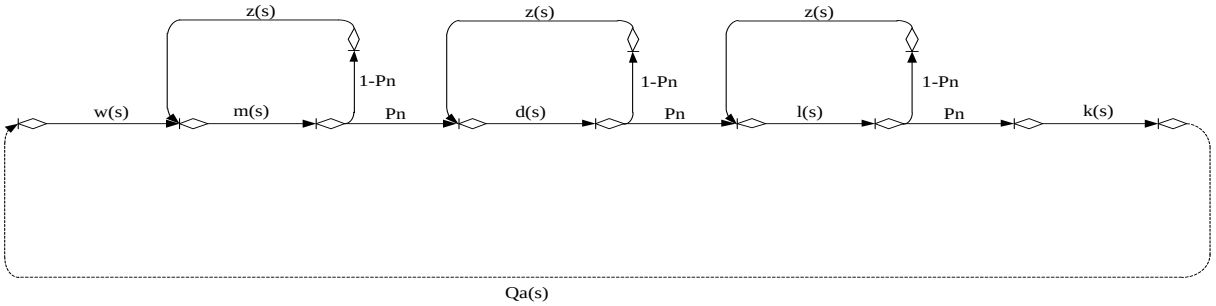

Рисунок 2.3 – Стохастическая сеть процесса реализации кибератаки «Сканирование сети и ее уязвимостей» на сетевые элементы БИС

Предполагая, что функции распределения времени реализации частных процессов относятся к классу экспоненциальных законов, получим (2.11):

$$\begin{cases} W(t) = 1 - e^{-wt}; \\ M(t) = 1 - e^{-mt}; \\ Z(t) = 1 - e^{-zt}; \\ D(t) = 1 - e^{-dt}; \\ L(t) = 1 - e^{-qt}; \\ K(t) = 1 - e^{-qt}; \end{cases} \tag{2.11}$$

Применяя преобразование Лапласа, получим (2.12).

$$\begin{aligned} w(s) &= \int_0^\infty e^{-st} d[W(t)] = \frac{w}{w+s}; \\ m(s) &= \int_0^\infty e^{-st} d[M(t)] = \frac{m}{m+s}; \\ z(s) &= \int_0^\infty e^{-st} d[Z(t)] = \frac{z}{z+s}; \\ d(s) &= \int_0^\infty e^{-st} d[D(t)] = \frac{d}{d+s}; \\ l(s) &= \int_0^\infty e^{-st} d[L(t)] = \frac{l}{l+s}; \\ k(s) &= \int_0^\infty e^{-st} d[K(t)] = \frac{k}{k+s}; \end{aligned} \tag{2.12}$$

Подставляя эти значения в ф.2.12 соответствующее значение $w(s); m(s); z(s); d(s) \cdot l(s) \cdot k(s)$, получаем окончательный вид эквивалентной функции: $w = \frac{1}{\overline{t}_{зап}}; \; m = \frac{1}{\overline{t}_{оп.элем}}; \; z = \frac{1}{\overline{t}_{повт}}; \; d = \frac{1}{\overline{t}_{оп.ос}}; l = \frac{1}{\overline{t}_{оп.серв}} k = \frac{1}{\overline{t}_{оп.уязв}}$.

Определим все петли k-го порядка:

Петли первого порядка: $m(s) \cdot (1 - P_n) \cdot z(s)$; $d(s) \cdot (1 - P_n) \cdot z(s)$; $l(s) \cdot (1 - P_n) \cdot z(s)$; $w(s) \cdot m(s) \cdot d(s) \cdot l(s) \cdot k(s) \cdot P_n^3 \cdot Q_a(s)$.

Петли второго порядка: $m(s) \cdot d(s) \cdot z(s)^2 \cdot (1 - P_n)^2$; $m(s) \cdot l(s) \cdot z(s)^2 \cdot (1 - P_n)^2$; $d(s) \cdot l(s) \cdot z(s)^2 \cdot (1 - P_n)^2$.

Петли третьего порядка: $m(s) \cdot d(s) \cdot l(s) \cdot z(s)^3 \cdot (1 - P_n)^3$.

С использованием топологического уравнения Мейсона, получаем общий вид эквивалентной функции стохастической сети:

$$H = 1 + \sum_{k=1}^{k} (-1)^k \cdot Q_k(s) = 0 \qquad (2.13)$$

где k – максимальный порядок петель, входящих в стохастическую сеть.

$Q_a(s) = \frac{1}{Q(s)}$ подставляя это значение в ф.(2.13), получаем общий вид эквивалентной функции стохастической сети (2.14):

$$Q(s) = \frac{w(s) \cdot m(s) \cdot d(s) \cdot l(s) \cdot k(s) \cdot P_n^3}{1 - z(s) \cdot (1 - P_n) \cdot [m(s) + d(s) + l(s)] + z(s)^2 \cdot (1 - P_n)^2 [m(s) \cdot d(s) + m(s) \cdot l(s) + d(s) \cdot l(s)] - z(s)^3 \cdot (1 - P_n)^3 \cdot m(s) \cdot d(s) \cdot l(s)} \qquad (2.14)$$

Определяем функцию распределения времени проведения КА типа «Сканирование сети и ее уязвимостей», для этого определим сначала начальные первые и вторые моменты (2.15).

$$\begin{aligned} M_1(s, P_n) &= (-1)^1 \cdot \frac{d}{ds} \left[\frac{Q(s, P_n)}{Q(s = 0, P_n)} \right] \\ M_2(s, P_n) &= (-1)^2 \cdot \frac{d^2}{ds^2} \left[\frac{Q(s, P_n)}{Q(s = 0, P_n)} \right] \end{aligned} \qquad (2.15)$$

юда среднее время реализации кибератаки равно (2.16):

$$\bar{t}_{\text{р}}(P_{\text{п}}) = -\frac{d}{ds}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0} \quad (2.16)$$

Дисперсия времени реализации кибератаки «Сканирование сети и ее уязвимостей» $D(\bar{t}_{\text{р}})$, определяемая как второй центральный момент, представлена выражением (2.17):

$$D(\bar{t}_{\text{р}}) = \frac{d^2}{ds^2}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0} - \left\{-\frac{d}{ds}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0}\right\}^2 \quad (2.17)$$

Вычисление математического ожидания и дисперсии позволяет с достаточной для инженерных расчетов точностью определить интегральную функцию распределения времени успешной реализации кибератаки «Сканирование сети и ее уязвимостей», как неполную Гамма-функцию (2.18):

$$F(t) = \begin{cases} 0, \text{ если } t < 0; \\ \int_0^t \frac{\mu^{\alpha}}{\Gamma(\alpha)} \cdot t^{\alpha-1} \cdot e^{-\mu \cdot t} dt, \text{ если } t > 0 \end{cases}, \quad (2.18)$$

где $\alpha = \frac{[\bar{t}_{\text{р}}(P_{\text{п}})]^2}{D(\bar{t}_{\text{р}})}$ - параметр формы; $\mu = \frac{\bar{t}_{\text{р}}(P_{\text{п}})}{D(\bar{t}_{\text{р}})}$ - параметр масштаба.

Результат: расчеты производились с использованием программного комплекса Mathcad-2014. По формуле (2.18) произведены расчеты, результаты которых представлены на рисунке 2.4. В качестве исходных данных использовались следующие значения среднего времени реализации частных процессов:

$\bar{t}_{зап} = 6\,мин;$ – среднее время запуска программно-аппаратного комплекса;

$\bar{t}_{оп.элем} = 7\,мин;$ – среднее время определение активных элементов БИС;

$\bar{t}_{оп.ос} = 9\,мин;$ – среднее время определение типов операционных систем (ОС) БИС;

$\bar{t}_{оп.серв} = 2\,мин;$ – среднее время определение сервисов БИС;

$\overline{t}_{оп.уязв} = 15\,мин$; – среднее время определение уязвимостей элементов БИС;

$\overline{t}_{повт} = 13\,мин$; – среднее время повторного запуска сетевого сканера элементов БИС;

$P_n = 0{,}1 \div 0{,}9$ – вероятность определения ОС активных элементов за среднее время соответственно $\overline{t}_{оп.элем}$, $\overline{t}_{оп.ос}$, $\overline{t}_{оп.серв}$.

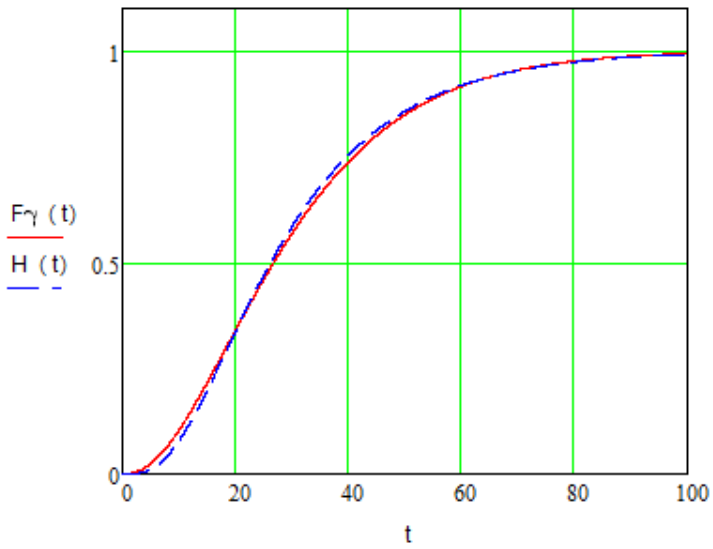

Рисунок 2.4 – Зависимость интегральной функции распределения вероятностей от времени реализации кибератаки «Сканирование сети и ее уязвимостей» при успешной реализации с вероятностью P_n

Вывод: в ходе данной работы был смоделирован процесс компьютерной атаки типа «Сканирование сети и ее уязвимостей». Для этого было произведено описание процесса атаки. На основе заданных исходных данных была построена стохастическая сеть обеспечивающая представление анализируемого процесса. Для полученной стохастической сети была определена эквивалентная функция. При определении функции распределения методом обращения, мы получаем наиболее точную оценку процесса реализации компьютерной атаки. По полученным графикам, представленным на рисунке 2.4, видно, что функции, полученные двумя различными методами, совпадают.

Профильная модель компьютерной атаки типа «DDoS-атаки».

Постановка задачи. С технической точки зрения БИС включают в себя: маршрутизаторы, коммутаторы, серверы, модемы и автоматизированные рабочие места (АРМ). Предположим, что сетевые элементы БИС функционируют в условиях DDoS-атак организованного злоумышленника. Под организованным нарушителем (злоумышленником) понимается группа людей, состоящая из высококвалифицированных специалистов в области информационной безопасности (ИБ), действующая по единому, согласованному во времени и месту плану и замыслу с целью нанесения ущерба БИС. На рисунке – 2.5 представлен принцип организации DDoS-атаки на сетевые элементы БИС. DDoS-атака основана на реализации множества отдельных DoS-атак за счет контроля нарушителем серверов, в которые нарушителем заблаговременно внедрены специальные программы агенты [6-13, 27-31, 50-56].

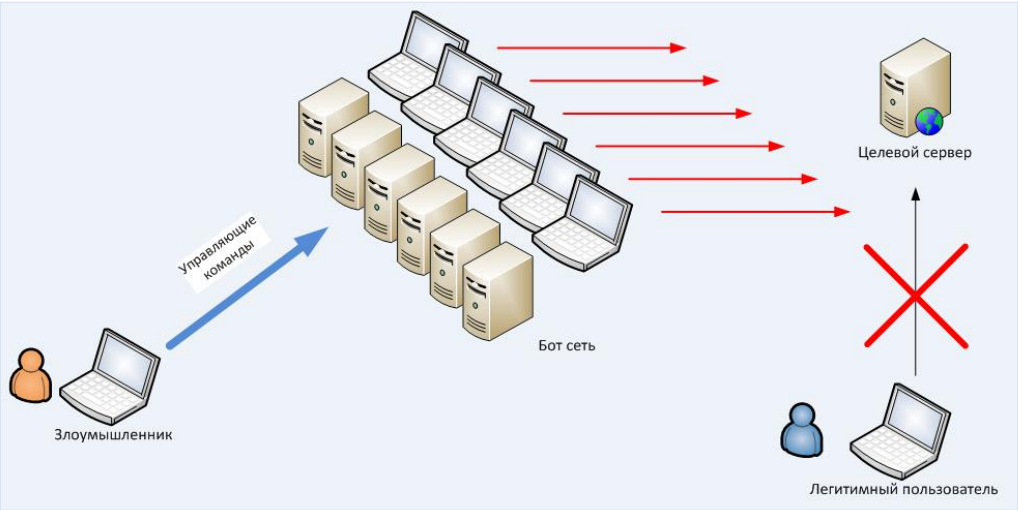

Рисунок 2.5 – Принцип реализации типовой DDoS-атаки на сетевые элементы БИС

При поступлении команды от компьютера злоумышленника, множество «зомби-компьютеров» обращаются с запросами к серверу, заставляя его реагировать на них, а эти «зомби-компьютеры» образуют «бот-сеть», то есть сеть зараженных узлов, которой управляет нарушитель. В результате, бот-сеть начинает обращаться с какими-либо запросами к целевой системе блокируя возможность ответа легитимным пользователям.

DDoS-атака считается успешной, если она привела к недоступности информационного ресурса для легитимных пользователей банка.

Для успешной реализации DDoS-атаки организованный нарушитель реализует следующие частные процессы, аналогично как в работе [6-13, 31, 48], кроме того, с вероятностью $(1-P_{\text{отп.запр}})$ на атакуемые сервера может быть направлен некорректный, специально подобранный запрос за некоторое время $\bar{t}_{\text{нек.запр}}$ с функцией распределения $O(t)$. В этом случае, при наличии ошибок в удаленной системе, возможно зацикливание процедуры обработки запроса, переполнение буфера с последующим «зависанием» сервера. Требуется определить интегральную функцию распределения вероятностей $F(t)$, среднее время $\bar{T}_p$ и коэффициент исправного действия сервера при реализации нарушителем DDoS-атаки.

При моделировании вводятся следующие ограничения и допущения:

– возможности организованного злоумышленника по доступу к элементам БИС, характеризуются указанными в постановке задачи вероятностными показателями;

– законы распределения случайного времени реализации частных процессов относится к классу экспоненциальных;

– значения вероятностей полагаются одинаковыми, т.е. $P_{\text{оп.элем}} = P_{\text{оп.ос}} = P_{\text{оп.серв}} = P_{\text{отп.запр}} = P_{\text{под.с}} = P_{\text{п}}$.

Решение:

Описанный в постановке задачи процесс реализации DDoS-атаки на сетевые элементы БИС представим в виде стохастической сети, приведенной на рисунке 2.6.

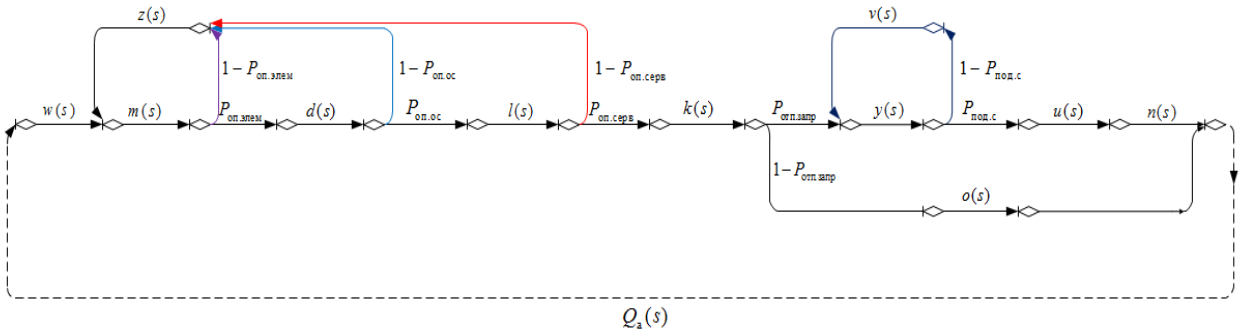

Рисунок 2.6 – Стохастическая сеть процесса реализации DDoS-атак на сетевые элементы БИС

В стохастической сети обозначено: $w(s)$, $m(s)$, $z(s)$, $d(s)$, $l(s)$, $k(s)$, $y(s)$, $o(s)$, $v(s)$, $u(s)$ и $n(s)$ – преобразования Лапласа-Стилтьеса соответствующих функций распределения, указанных в постановке задачи и определяемых как (2.19):

$$r_i(s) = \int_0^{\infty} \exp(-st) d[R_i(t)] = \frac{r_i}{r_i + s} \qquad (2.19)$$

С целью определения эквивалентной функции стохастической сети (рис.2.6) замкнем вход и выход стохастической сети фиктивной ветвью $Q_a(s) = \frac{1}{Q(s)}$ и перечислим петли первого и второго порядков [6-13, 31, 48]:

Петли первого порядка:

$\text{loop1}_1 := m(s) \cdot (1 - P_n) \cdot z(s)$;

$\text{loop1}_2 := m(s) \cdot d(s) \cdot P_n \cdot (1 - P_n) \cdot z(s)$;

$\text{loop1}_3 := m(s) \cdot d(s) \cdot l(s) \cdot P_n^{\,2} \cdot (1 - P_n) \cdot z(s)$;

$\text{loop1}_4 := y(s) \cdot (1 - P_n) \cdot v(s)$;

$\text{loop}_{общ1} := w(s) \cdot m(s) \cdot d(s) \cdot l(s) \cdot k(s) \cdot y(s) \cdot u(s) \cdot n(s) \cdot P_n^5$;

$\text{loop}_{общ2} := w(s) \cdot m(s) \cdot d(s) \cdot l(s) \cdot k(s) \cdot o(s) \cdot (1 - P_n) \cdot P_n^3$

Петли второго порядка:

$\text{loop2}_1 := m(s) \cdot (1 - P_n)^2 \cdot z(s) \cdot y(s) \cdot v(s)$;

$\text{loop2}_2 := m(s) \cdot d(s) \cdot P_n \cdot (1 - P_n)^2 \cdot z(s) \cdot y(s) \cdot v(s)$;

$\text{loop2}_3 := m(s)\cdot d(s)\cdot l(s)\cdot P_{\text{п}}{}^2\cdot(1-P_{\text{п}})^2\cdot z(s)\cdot y(s)\cdot v(s)$.

С использованием уравнения Мейсона $H = 1+\sum_{i=1}^{k}(-1)^k\cdot Q_k(s) = 0$, где $Q_k(s)$ - эквивалентные функции петель k-го порядка, определим эквивалентную функцию стохастической сети (2.20):

$$Q(s,P_{\text{п}}) = \frac{w(s)\cdot m(s)\cdot d(s)\cdot l(s)\cdot k(s)\cdot y(s)\cdot u(s)\cdot n(s)\cdot P_n^5}{1-m(s)\cdot(1-P_{\text{п}})\cdot z(s)\cdot\left[1+d(s)\cdot P_{\text{п}}+d(s)\cdot l(s)\cdot P_{\text{п}}^2\right]-y(s)\cdot(1-P_{\text{п}})\cdot v(s)+}$$

$$+\frac{}{+m(s)\cdot(1-P_{\text{п}})^2\cdot z(s)\cdot y(s)\cdot v(s)\cdot\left[1+d(s)\cdot P_{\text{п}}+d(s)\cdot l(s)\cdot P_{\text{п}}^2\right]}+\frac{w(s)\cdot m(s)\cdot d(s)\cdot l(s)\cdot k(s)\cdot o(s)\cdot(1-P_{\text{п}})\cdot P_n^3}{1-m(s)\cdot(1-P_{\text{п}})\cdot z(s)\cdot\left[1+d(s)\cdot P_{\text{п}}+d(s)\cdot l(s)\cdot P_{\text{п}}^2\right]} \quad (2.20)$$

Так как (2.20), по определению, является характеристической функцией, то ее дифференцирование позволяет найти первый и второй начальные моменты случайного времени реализации моделируемого процесса, т.е.

$$M_1(s,P_{\text{п}}) = -\frac{d}{ds}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0},$$

$$M_2(s,P_{\text{п}}) = \frac{d^2}{ds^2}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0}$$

здесь среднее время реализации DDoS-атаки равно:

$$\overline{t}_{\text{р}}(P_{\text{п}}) = -\frac{d}{ds}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0}$$

Дисперсия времени реализации DDoS-атаки $D(\overline{t}_{\text{р}})$, определяемая как второй центральный момент, представлена выражением

$$D(\overline{t}_{\text{р}}) = \frac{d^2}{ds^2}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0} - \left\{-\frac{d}{ds}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0}\right\}^2$$

Вычисление математического ожидания и дисперсии позволяет с достаточной для инженерных расчетов точностью определить интегральную функцию распределения времени успешной реализации DDoS-атаки, как неполную Гамма-функцию [6-13, 31]:

$$F(t)=\begin{cases}0, \text{ если } t<0;\\ \int_0^t \frac{\mu^{\alpha}}{\Gamma(\alpha)}\cdot t^{\alpha-1}\cdot e^{-\mu\cdot t}dt, \text{ если } t>0\end{cases}, \quad (2.21)$$

где $\alpha=\frac{[\bar{t}_{\text{р}}(P_{\text{п}})]^2}{D(\bar{t}_{\text{р}})}$ - параметр формы; $\mu=\frac{\bar{t}_{\text{р}}(P_{\text{п}})}{D(\bar{t}_{\text{р}})}$ - параметр масштаба.

Расчеты производились с использованием программного комплекса Mathcad-2014. По формуле (2.21) произведены расчеты, результаты которых представлены на рисунке 2.7. В качестве исходных данных использовались следующие значения среднего времени реализации частных процессов: $\bar{t}_{\text{зап}}=2\,\text{мин.}$, $\bar{t}_{\text{оп.элем}}=7\,\text{мин.}$, $\bar{t}_{\text{оп.ос}}=5\,\text{мин.}$, $\bar{t}_{\text{оп.серв}}=6\,\text{мин.}$, $\bar{t}_{\text{оп.уязв}}=7\,\text{мин.}$, $\bar{t}_{\text{повт.ск}}=4\,\text{мин.}$, $\bar{t}_{\text{запр}}=4\ \text{мин.}$, $\bar{t}_{\text{дос.к серв.}}=1\,\text{мин.}$, $\bar{t}_{\text{пов.запр}}=4\,\text{мин.}$, $\bar{t}_{\text{завис}}=3\,\text{мин.}$, $\bar{t}_{\text{нек.запр}}=3\,\text{мин.}$ а значения вероятностей изменялось в пределах $P_{\text{п}}=0,7\div0,9$.

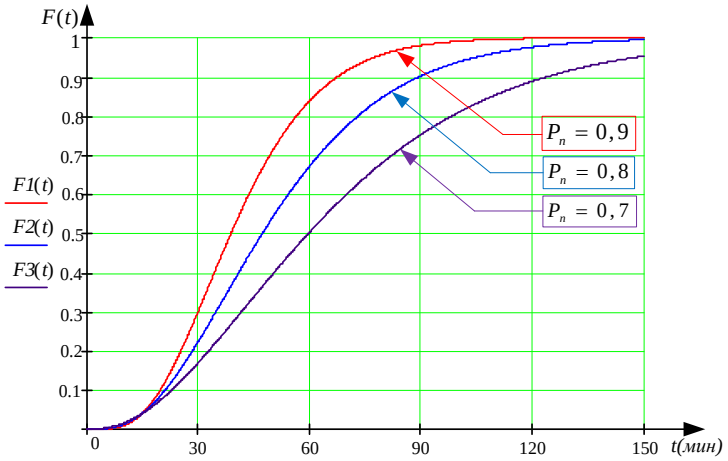

Рисунок 2.7 – Зависимость интегральной функции распределения вероятностей от времени реализации DDoS-атаки при успешной реализации с вероятностью $P_{\text{п}}$

В свою очередь, среднее время реализации DDoS-атаки при различных значениях $P_{\text{п}}$ составляет: при $P_{\text{п}}=0,7$, $\bar{T}_{p}=64,445\,мин.$; при $P_{\text{п}}=0,8$, $\bar{T}_{p}=50,197\,мин.$, а при $P_{\text{п}}=0,9$ $\bar{T}_{p}=41,129\,мин.$

Коэффициент исправного действия сервера (сетевых элементов) определим как (2.22):

$$K_{и.д.серв}(t)=\frac{T_{И}(t)}{T_{И}(t)+T_{В}}, \quad (2.22)$$

где: $T_{И}(t)=\dfrac{1-F(t)}{f(t)}=\dfrac{1-\int_0^t \dfrac{\mu^{\alpha}}{\Gamma(\alpha)}\cdot t^{\alpha-1}\cdot e^{-\mu\cdot t}dt}{\dfrac{\mu^{\alpha}}{\Gamma(\alpha)}\cdot t^{\alpha-1}\cdot e^{-\mu\cdot t}}$ – среднее время исправной работы;

$T_{В}=0{,}5\ ч$ среднее время восстановления сервера (сетевых элементов) после отказа, согласно [6-13, 31, 48].

Изменение коэффициента исправного действия сервера при $T_{В}=0{,}5\ ч$ и различных значениях вероятности $P_{\text{п}}$ показана рисунке 2.8.

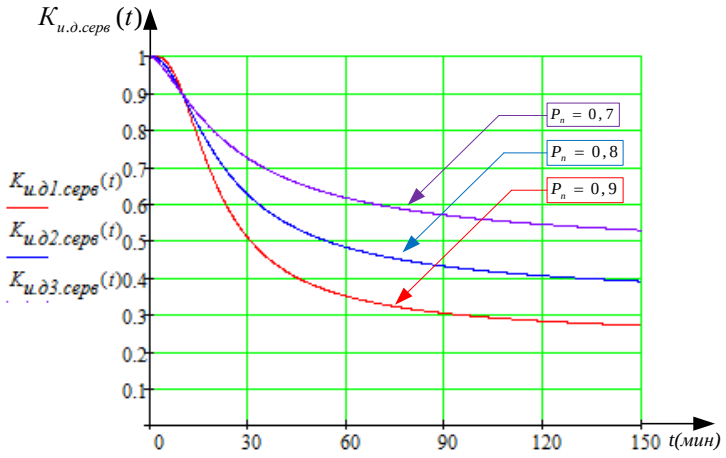

Рисунок 2.8 – График коэффициента исправного действия сервера при различных значениях вероятности $P_{\text{п}}$

Анализ полученных результатов позволяет сделать следующие выводы:

– разработанная модель является работоспособной, чувствительной к изменению исходных данных, адекватно отображает процесс реализации DDoS-атак и дает возможность определить вероятностно-временные характеристики системы кибервоздействия злоумышленника;

– полученные результаты могут быть использованы в ходе комплексной оценки устойчивости функционирования БИС;

– особенностью представленной модели является то, что она является укрупненной и учитывает полученные ранее результаты моделирования процессов сканирования портов и идентификации сервисов, определения типа (версии) операционных систем (ОС) и уязвимости узлов [6-14].

Результаты моделирования показывают, что основное влияние на успешность реализации нарушителем DDoS-атаки на сетевые элементы БИС оказывают параметры, отображающие его доступность к сетевым элементам, применяемые в БИС методы идентификации и аутентификации легитимных пользователей, а также уровень подготовки (квалификации) злоумышленника.

2.3. Метод оценки качества функционирования сетевых элементов БИС в условиях DDoS-атак злоумышленника. Актуальность обусловлена возможностью срыва банковских операций за счет воздействия на элементы БИС DDoS атак злоумышленника. На основе математического аппарата GERT-сетей предлагается подход к оценке качества функционирования сетевых элементов БИС, сущность которого заключается в представлении процесса обслуживания потока данных сетевых элементов в условиях DDoS атак злоумышленника в виде стохастической сети, задании вида частных распределений, определении эквивалентной функции с последующим определением функции распределения времени задержки пакетов данных. Предлагаемая модель позволяет производить оценку качества функционирования сетевых элементов в условиях DDoS атак злоумышленника как при передаче стационарного Пуассоновского, так и самоподобного трафика, представляемого моделями потоков Вейбулла и Парето. Модель позволяет анализировать и вырабатывать направления по повышению качества функционирования сетевых элементов БИС в условиях деструктивного информационного воздействия злоумышленника. Значительное влияние качества функционирования БИС на эффективность банковско-финансовых организаций, с одной стороны, определяет высокие требования к элементам БИС, а с другой - повышенное внимание к ним со стороны нарушителей, целью которых являются автоматизированные системы управления банковскими процессами. Реализуя компьютерные атаки на сетевые элементы БИС, злоумышленники нарушают штатную

работу элементов БИС, а значит, внедряемые системы БИС должны не только обеспечивать банковские операции, но и соответствовать высоким требованиям по кибербезопасности, как элементов автоматизированных систем управления, так и телекоммуникационных сетей. Как показал анализ [6-17], наиболее эффективным и самым реализуемым видом кибервоздействия на автоматизированные системы управления и элементы БИС являются DDoS атаки на сетевые элементы, приводящие к существенной задержке или блокированию обслуживаемого корпоративной сети. Поэтому актуализируется задача оценки качества функционирования сетевые элементы БИС в условиях воздействия DDoS атак злоумышленника.

С целью разработки механизма учета воздействий DDoS атак на сетевые элементы, проведем краткий обзор существующих подходов к оценке качества функционирования современных сетей передачи данных, используемых для обеспечения устойчивой работы автоматизированных систем управления технологическими процессами. Это позволяет выделить среди множества показателей качества функционирования сетевых элементов, нормируемых рекомендациями ITU-T, ETSI, 3GPP, IETF и существующими отечественными руководящими документами, только те показатели, которые согласуются с требованиями, предъявляемыми со стороны системы управления технологическими процессами к процессу информационного обмена. Среди таких показателей можно выделить следующие: производительность и масштабируемость сети, характеризуемая средней скоростью передачи данных; вероятность потери данных, оцениваемая по значению вероятности потери пакетов; среднее время и джиттер времени задержки данных. При этом разрабатываемый механизм должен учитывать кибервоздействие на сетевые элементы, а также случайный характер передаваемых в современных БИС технологического назначения потоков и их особенности, среди которых основными являются существенная нестационарность и пульсации с долговременными зависимостями, объясняемые наличием у потока данных свойства

самоподобия (фрактальности) [16-18, 31, 48]. В работах [17-20, 41] предлагается способ расчета вероятности потери пакетов, основанный на использовании фундаментальных выражений, полученных для систем массового обслуживания M/M/1 с учетом категоричности потока и дисциплины обслуживания заявок с введением поправочных коэффициентов, учитывающих вариативность трафика [42], индекса Херста [17, 41, 42] и связанных с ним параметров [10,11,12]. Данные работы, безусловно, вносят заметный вклад в развитие методов теории телетрафика, однако не учитывают влияние на потери пакетов результатов реализации нарушителем компьютерных атак.

Работы [17-20] ориентированы на расчет вероятностно-временных характеристик БИС и ее элементов, таких как средняя скорость передачи данных, среднее время ожидания обслуживания и джиттер времени задержки. При этом основное внимание при расчете указанных величин уделяется учету самоподобности передаваемого потока данных. Наиболее полно, по нашему мнению, проведен анализ методов расчета в [22], где приведены соотношения для определения функций распределения времени задержки данных, учитывающие категоричность передаваемых потоков и их самоподобие. Однако, приведенные в данных работах результаты не учитывают влияние на значение вычисляемых величин результатов реализации нарушителем DDoS атак. Для оценки качества функционирования БИС и оценки антивирусной защиты корпоративных сетей, в [24, 46] предложено использование комплекса GERT-моделей. Основным ограничением полученных в [24] решений является ограничение на вид передаваемого в сети трафика.

Постановка задачи.

Пусть имеется корпоративная сеть, функционирующая в условиях угрозы реализации нарушителем DDoS-атаки и состоящая из канала передачи данных с пропускной способностью $R\left[\text{бит}/c\right]$, входных

накопителей (буферов памяти) объемом $0 < K < \infty$ и устройства управления. На БИС поступает суммарный поток пакетов, имеющих объем $V[бит]$ и интенсивностью $\lambda_{вх.\Sigma} = \sum_{i=1}^{n} \lambda_i$ т.е. на каждый из n входов поступает поток пакетов с интенсивностью λ_i, $i = \overline{1,n}$, а вероятность поступления данных на $i-й$ вход равна $P_i = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i}$, $i = \overline{1,n}$. Если канал передачи не занят обслуживанием и $i-й$ буфер памяти не полностью заполнен ранее поступившими пакетами данных, а вероятность этого события равна $(1 - P_{пот.i})$, $i = \overline{1,n}$ поступивший пакет после некоторого ожидания в течение времени $t_{ож.i}$ с функцией распределения $W(t)$ будет успешно обслужен (передан) за случайное время $t_{оп} = \frac{V}{R}$ с функцией распределения $B(t)$. В противном случае, а вероятность этого события равна $P_{пот.i}$, $i = \overline{1,n}$, пакет данных получит отказ в обслуживании, т.е. будет потерян и через некоторое время ожидания подтверждения получения данных корреспондентом $t_к$ с функцией распределения $D(t)$ вновь поступит на $i-й$ вход узла коммутации. Положим, что корпоративная сеть доступна компьютерной разведке злоумышленника, который вероятностью $P_{КА}$ успешно реализует DDoS атаку. В ходе компьютерной атаки (КА) на корпоративную сеть поступает дополнительный поток пакетов с суммарной интенсивностью $\lambda_{КА}$, который равномерно распределяется между входами элементов и приводит к переполнению накопителей, а также потере пакетов данных.

Требуется определить функцию распределения и среднее время задержки пакетов данных в корпоративной сети, функционирующей в условиях реализации нарушителем DDoS атаки.

Ограничения и допущения:

– оборудование, входящее в состав корпоративной сети технически исправно;

– входящий поток пакетов характеризуется распределением Вейбулла или Парето;

– время ожидания и длительности обслуживания характеризуются гамма- распределением, а время ожидания корреспондентом подтверждения о получении данных – экспоненциальным.

Решение:

Представим описанный в постановке задачи процесс в виде стохастической сети (рис.2.9).

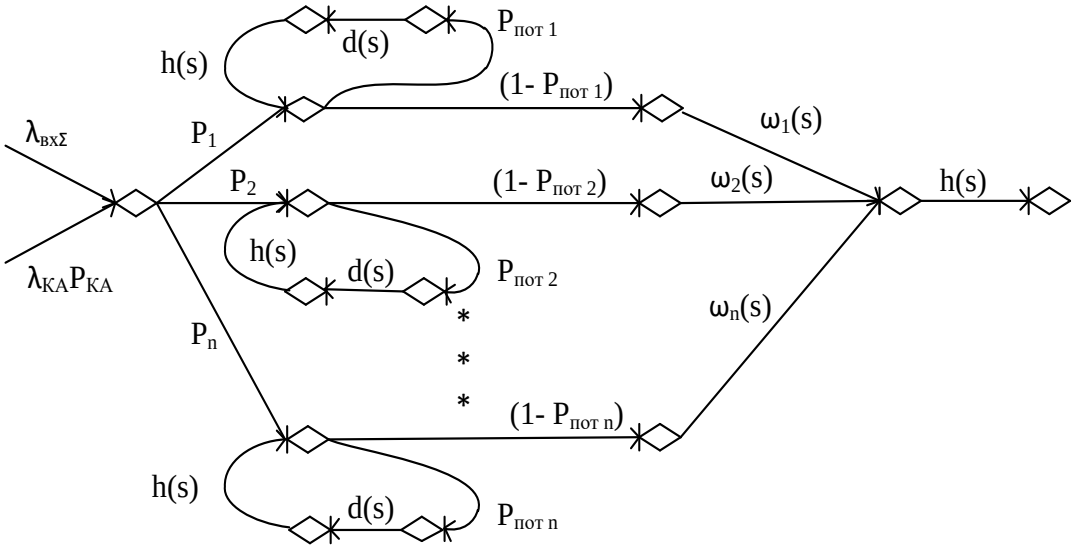

Рисунок 2.9 – Стохастическая сеть процесса обслуживания потока пакетов узлом коммутации в условиях DDoS атаки злоумышленника

На рисунке обозначено: $h(s)$, $\omega_i(s)$, $d(s)$ – преобразование Лапласа – Стилтьеса функций распределения времени передачи пакета данных $B(t)$, ожидания передачи (обслуживания) в $i-м$ накопителе $W_i(t)$ и времени ожидания подтверждения получения данных от корреспондентов $D(t)$, соответственно, определяемых как $f(s)=\int_0^{\infty}\exp(-sT)d\left[F(t)\right]$.

Используя уравнение Мейсона [31, 48] для замкнутых графов с учетом принятых допущений на вид частных функций распределений, получим эквивалентную функцию стохастической сети (2.23):

$$Q(S)=\sum_{i=1}^{n}\frac{P_i\cdot\left(1-P_{nom.i}\right)\cdot\omega_i^{\alpha_i}\cdot\mu^{\beta}\cdot(d+s)}{(\mu+s)^{\beta}\cdot(s+\omega_i)^{\alpha_i}\cdot\left[(d+s)(\mu+s)^{\beta}-P_{nom.i}\cdot d\cdot\mu^{\beta}\right]} \qquad (2.23)$$

где $P_i=\dfrac{\lambda_i+\frac{\lambda_{KA}\cdot P_{KA}}{n}}{\sum_{i=1}^{n}\lambda_i+\lambda_{KA}\cdot P_{KA}}$ – вероятность поступления пакета данных на $i-й$ вход узла коммутации. $d=\dfrac{1}{t_k}$; $\mu=\dfrac{T_{оп}}{D_{оп}}$; $\beta=\dfrac{T_{оп}^{\ 2}}{D_{оп}}$; $\omega_i=\dfrac{\overline{t_{ожі}}}{D_{ожі}}$; $\alpha_i=\dfrac{\overline{t_{ожі}}^{2}}{D_{ожі}}$, $P_{КА}$ – вероятность доступности сетевых элементов и успешной реализации нарушителем DDoS атаки, определяемая методами [25, 46]. $T_{оп}$, $D_{оп}$ – среднее и дисперсия времени передачи пакета данных. $\overline{t_k}$ – среднее время ожидания подтверждения получения данных.

$\overline{t_{\text{ож}i}}=\dfrac{\rho_i\left(1-\rho_i^{\frac{K}{C}+1}\right)C\left[1-\rho_i^{K}(K+1)+K\rho_i^{K+1}\right]}{\left(1-\rho_i^{\frac{K}{C}+2}\right)b(1-\rho_i)(1-\rho_i^{K+1})}$ – среднее время ожидания передачи [19-22];

$D_{\text{ож}i}=\dfrac{T_{\text{оп}}{}^{2}C^{2}\rho_i\left[2(1-\rho_i{}^{K})+K\rho_i{}^{K}(1-\rho_i)[\rho_i(K+1)-K-3]\right]}{(1-\rho_i)(1-\rho_i{}^{K+2})}-\overline{t_{\text{ож}i}}^{2}$ – дисперсия времени ожидания передачи [19-23];

$\rho_i=\dfrac{\lambda_i+\frac{\lambda_{KA}P_{KA}}{n}}{b}$ – интенсивность входящей на i-й вход корпоративной сети; $C=\dfrac{C_a^2+C_b^2}{2}$ – среднеквадратичный коэффициент вариации; C_b^2 – квадратичный коэффициент вариации времени передачи (обслуживания) пакета данных, равный «1» при переменной и «0» - при фиксированной длине пакета; C_a^2 – квадратичный коэффициент вариации входящего потока пакетов, численно равный:

$C_a^2 = C_{aw}^2 = \frac{\Gamma\left(1+\frac{2}{\alpha}\right)}{\Gamma\left(1+\frac{1}{\alpha}\right)^2} - 1$ – при потоке Вейбулла с параметром формы распределения, равным $\alpha = (2 - 2H)$;

$C_a^2 = C_{ap}^2 = \left[\frac{\chi_{max}^2 \chi_{min}^{\alpha} - \chi_{max}^{\alpha} \chi_{min}^2}{2-\alpha} - \frac{\alpha\left(\chi_{max}^1 \chi_{min}^{\alpha} - \chi_{max}^{\alpha} \chi_{min}^1\right)^2}{(1-\alpha)^2\left(\chi_{max}^{\alpha} - \chi_{min}^{\alpha}\right)}\right] *$

$\frac{(1-\alpha)^2(\chi_{max}^{\alpha} - \chi_{min}^{\alpha})^2}{\chi_{max}^1 \chi_{min}^{\alpha} - \chi_{max}^{\alpha} \chi_{min}^1}$ – при потоке Парето с параметром формы распределения, равным $\alpha = (3 - 2H)$, [22]; Н- индекс Херста; $\chi_{мин}$, $\chi_{мах}$ – минимальное и максимальное значение величины, характеризующей размеры пачек пакетов в потоке Парето.

$P_{\text{пот}i} = \frac{(1-\rho_i)}{1-\rho_i^{(K+1)^{2(1-H)}}} \rho_i^{K^{2(1-H)}}$ – вероятность потери (отказа в обслуживании) пакета, [31, 48].

Для определения функции распределения используем метод двух моментной аппроксимации [31, 48], для чего найдем первый начальный и второй центральный моменты времени задержки пакетов данных (2.24-2.25):

$$M_1 = T = -\frac{d}{ds}\left\{\frac{Q(s)}{Q(0)}\right\}_{s=0} = \sum_{i=1}^{n} P_i \left[\overline{t_{\text{ож}i}} + \frac{t_{\text{оп}} + t_k P_{\text{пот}i}}{1 - P_{\text{пот}i}}\right] \quad (2.24)$$

$$\dot{M}_2 = D = \frac{d^2}{ds^2}\left\{\frac{Q(s)}{Q(0)}\right\}_{s=0} - M_1^2 = \\ = D_{\text{оп}} + \sum_{i=1}^{n} P_i \left[D_{\text{ож}i} + (t_k + t_{\text{оп}})^2 \left[\frac{1}{(1 - P_{\text{пот}i})^2} - 1\right]\right] \quad (2.25)$$

Тогда функция распределения времени задержки данных в корпоративной сети имеет вид (2.26):

$$F(t) = \frac{(h)^a}{\Gamma(a)} \int_0^t x^{a-1} \, exp\{-ht\} \, dx \quad (2.26)$$

где: $a = \frac{M_1^2}{\dot{M}_2}; h = \frac{M_1}{\dot{M}_2}$ – параметры формы и масштаба гамма распределения.

В свою очередь средняя вероятность потери пакетов данных в корпоративной сети (2.27-2.28):

$$\overline{P_{\text{пот}}} = \sum_{i=1}^{n} P_i P_{\text{пот}i} \quad (2.27)$$

$$\overline{P_{\text{пот}}} = \sum_{i=1}^{n} P_i P_{\text{пот}i} \quad (2.28)$$

а вариация времени задержки пакетов в корпоративной сети (2.29):

$$Var = \frac{\sqrt{D}}{T} \quad (2.29)$$

Таким образом, поставленная задача решена.

По полученным соотношениям (ф.2.27-2.29) произведены расчеты, результаты которых представлены на рис.2.10.

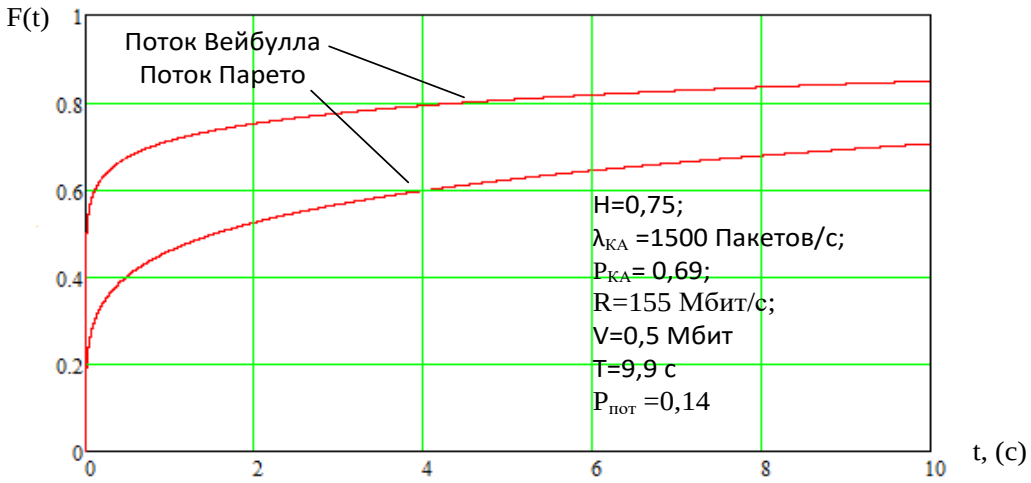

Рисунок 2.10 – Графики функций распределения времени задержки пакетов на корпоративной сети, функционирующей в условиях DDoS атак злоумышленника

При расчетах предполагалось: пропускная способность канала передачи $R = 155 \, Мбит/с$; средний объем пакетов $V = 0,5 \, Мбайт$; узел коммутации имеет три входа $n = 3$; емкости накопителей $K = 50$; интенсивность потоков данных на входах УК $\lambda_1 = 50 \, пакетов/с$; $\lambda_2 = 45 \, пакетов/с$; $\lambda_3 = 55 \, пакетов/с$; суммарная интенсивность атакующего потока данных $\lambda_{КА} = 1500 \, пакетов/с$; вероятность доступности УК и успешной

реализации нарушителем компьютерной атаки $P_{KA} = 0,69$; входящие потоки данных характеризуются распределениями Вейбулла и Парето, и индексом Херста $H = 0,75$.

Вывод: на основании общих принципов построения и функционирования современных корпоративных сетей и обеспечения качества предоставляемых услуг пользователям при передаче разнородного трафика в статье предложена модель функционирования корпоративной сети передачи данных в условиях DDoS атак злоумышленника при произвольных распределениях времени поступления пакетов. Модель основана на представлении процесса обслуживания пакетов данных на корпоративной сети в виде стохастической сети, определении ее эквивалентной функции, с последующим определением функции распределения времени задержки данных.

2.4. Математическая модель процесса функционирования БИС на базе IP-технологии в условиях кибервоздействий.

Постановка задачи: Пусть имеется корпоративная сеть на базе IP-технологии, в которой передаются пакеты, состоящие из заголовка IP и кадра данных, сформированного из используемого кодека. В таблице 2.1 приведены средние субъективные оценки качества различных методов кодирования.

Таблица 2.1 – Основные характеристики кодеков

Кодек	**Скорость передачи, кбит/с**	**MOS**	**Размер кадра, мс**
G.711 PCM	64	4,3	0,125
G.726 Multi-rate ADPCM	16-40	2-4,3	0,125
G.723 MP-MLQ ACELP	5,3	3,7	30
G.728 LD-CEL	16	4,1	0,625
G.729 CS-ACELP	8	4,0	10

При организации корпоративной сети, маршрут передачи определяются в соответствии с учетом качеством обслуживания. Все входящие маршруты содержит m узлов, а также $m-1$ участков, по которых могут осуществляться компьютерные атаки (КА) [6-13]. Время передачи данных определено по $t_{пер} = V/R$ [27-30], на участке с отношением объема V передаваемых информаций к скорости передачи R (2.30):

$$t_{пер,i} = \lim_{\lambda \to 0} \left[\sum_{i=1}^{n-1} \frac{1}{\mu_i} \cdot \frac{1-(K_i+1)\cdot \rho^{K_i} + K_i \cdot \rho^{K_i+1}}{(1+\rho^{K_i})\cdot(1-\rho)} \right] = \sum_{i=1}^{n-1} \frac{1}{\mu_i} \quad при \;\; R = const, \qquad (2.30)$$

где K_i – ёмкость накопителя на i-м узле сетевом элементе; $\rho = \frac{\lambda_i}{\mu_i}$ – входящая нагрузка, численная равная отношению интенсивностей поступления пакетов передачи λ_i к их обслуживанию μ_i (т.е. передачи на i-м участке маршрута передачи); $m-1$ – количество участков на маршруте, на котором находится m узлов.

Предположим, что на корпоративную сеть осуществляется деструктивное информационное воздействие, в ходе которого нарушитель может успешно реализовать n видов КА, каждая из которых с вероятностью P_i; $i = \overline{1,n}$ нарушает работоспособность сети, т.е. создает условия, при которых качество передачи пакетов снижается ниже допустимого уровня. Если сеть не прерывается, пакеты данных будут передаваться с течением времени $t_{пер}$. В общем случае $t_{пер}$ является случайной величиной с функцией распределения (ФР) $B(t)$. В случае нарушения работоспособности сеть восстанавливается за случайное время $t_{в_i}$; $i = \overline{1,n}$ с ФР времени восстановления $\Delta_i(t)$, а поступивший пакет данных передается повторно. Входящий поток пакетов данных является редкоследующим [31, 48], при котором вероятность поступления очередного пакета в момент обслуживания предыдущего пренебрежимо мала, то есть при случайном времени обслуживания интенсивность такого потока стремится к нулю. КА на сеть -IP возможны как во время передачи

пакетов, так и в паузах между ними [31, 48], количество мест для ожидания передачи считается неограниченным. Требуется определить математическое ожидание $\overline{T}_h$ и функцию распределения времени успешной передачи пакетов данных в условиях *n* видов КА. Представим описанный в постановке задачи процесс функционирования телефонной IP-сети в виде стохастической сети (рис. 2.11).

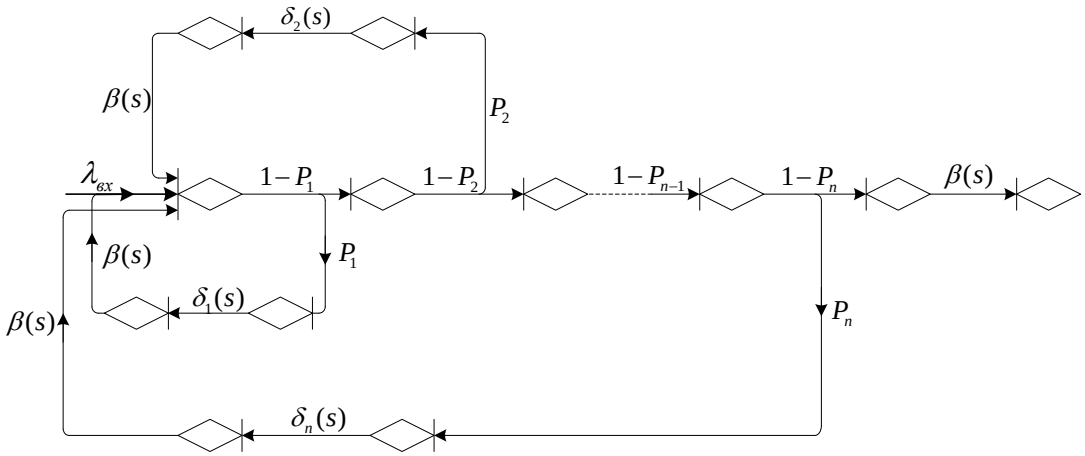

Рисунок 2.11 – Стохастическая сеть процесса функционирования сети IP в условиях *n*-го вида КА нарушителя

В стохастической сети указывается: $\beta(s)$ и $\delta_i(s)$ – преобразования Лапласа–Стилтьеса соответствующих функций распределения, которые означают значение ФР времени передачи пакетов без учета КА нарушителя, т. е. в «идеальных условиях» и ФР времени восстановления после *i*-го вида КА (2.31):

$$\beta(s) = \int_0^\infty e^{-st} d[B(t)];$$

$$\delta_i(s) = \int_0^\infty e^{-st} d[\Delta_i(t)], \quad i = \overline{1,n} \ . \tag{2.31}$$

С использованием уравнения Мейсона для замкнутых графов [6-13, 31, 48] составим эквивалентную функцию стохастической сети (2.32):

$$h_n(s)=\frac{k\beta(s)\left(\bar{d}+\bar{c}+s\right)\cdot\prod_{i=1}^{n}\left(1-P_i\right)}{\left[1-\beta(s)\sum_{i=1}^{n}P_i\delta_i(s)\prod_{j=1}^{i-1}\left(1-P_j\right)\right]\left(\bar{d}+s\right)}=\frac{V(s)}{U(s)},\qquad(2.32)$$

где $\bar{d}=\sum_{i=1}^{n}t_{\text{в}i}^{-1}P_i;\quad \bar{c}=\sum_{i=1}^{n}t_{p\text{в}i}^{-1}P_i$ – математические ожидания интенсивностей восстановления и реализации нарушителем КА соответственно;

$k=\frac{\bar{d}}{\bar{d}+\bar{c}}$ – вероятность восстановления работоспособности сетевых элементов за время повторной передачи пакета и реализации очередной КА.

Для получения математического ожидания и функции распределения времени передачи необходимо вычислить значение производных многочленов числителя и знаменателя (2.3) в точке $s=0$ (2.33):

$$V'(s)=k\cdot\prod_{i=1}^{n}\left(1-P_i\right)\left[\beta'(s)\left(\bar{d}+\bar{c}+s\right)+\beta(s)\left(\bar{d}+\bar{c}\right)\right];$$

$$V'(0)=k\left(\bar{d}+\bar{c}\right)\left(1-\overline{t_\beta}\right)\cdot\prod_{i=1}^{n}\left(1-P_i\right);\qquad(2.33)$$

$$U'(s)=d\left[1-\beta(s)\sum_{i=1}^{n}P_i\delta_i(s)\prod_{j=1}^{i-1}\left(1-P_j\right)\right]+$$
$$+\left(\bar{d}+s\right)\left[-\beta'(s)\sum_{i=1}^{n}P_i\delta_i(s)\prod_{j=1}^{i-1}\left(1-P_j\right)-\beta(s)\sum_{i=1}^{n}P_i\delta_i'(s)\prod_{j=1}^{i-1}\left(1-P_j\right)\right]$$

$$U'(0)=\bar{d}\left[1-\left(1-\overline{t_\beta}\right)\sum_{i=1}^{n}P_i\prod_{j=1}^{i-1}\left(1-P_j\right)+\sum_{i=1}^{n}P_i\overline{t_{\delta i}}\prod_{j=1}^{i-1}\left(1-P_j\right)\right].\qquad(2.34)$$

Математическое ожидание времени передачи пакета в условиях КА определяется как (2.35):

$$\overline{T}_h=\frac{-d}{ds}\left[\frac{h_n(s)}{h_n(0)}\right]_{s=0}.\qquad(2.35)$$

Заменив

$$\overline{P}=\prod_{i=1}^{n}(1-P_i);\qquad \overline{E}=1-\sum_{i=1}^{n}P_i\prod_{j=1}^{i-1}(1-P_i),\tag{2.36}$$

получим ф. 2.36 в виде:

$$\overline{T}_h=\frac{\overline{P}}{\left(1-\overline{E}\right)^2}\cdot\left[\sum_{i=1}^{n}P_i\overline{t_{\delta i}}\cdot\prod_{j=1}^{i-1}\left(1-P_j\right)+\bar{t}_{\beta}\right].$$

Соответственно, дисперсия определяется по формуле [6-13, 31, 48]

$$D\left[t_h\right]=h_1-h_1^2=\frac{d^2}{ds^2}\left[\frac{h_n(s)}{h_n(0)}\right]_{s=0}-\left[\frac{d}{ds}\left[\frac{h_n(s)}{h_n(0)}\right]_{s=4}\right]^2.\tag{2.37}$$

Необходимо произвести обратной процесс на получение функция распределения времени передачи пакетов, позволяющее вычислить оригинал $H_n(t)$ по его изображению $h_n(s)$ [6-13, 31, 48]. Для демонстрации изложенного метода определения функции распределения времени доведения пакетов данных в IP сети рассмотрим следующую частную задачу.

Постановка частной задачи: предполагаем, что целью нарушителя состоит в том, чтобы заблокировать оборудование соответствующих узлов сети-IP, на которые нарушитель осуществляет КА и нарушает их работоспособность с вероятностью P_1 и P_2 соответственно. Если работоспособность узлов не нарушена, то пакет, поступивший на вход канала связи, будет передан за время $t_{пер}$, которое определяется технической скоростью передачи R и объемом V передаваемых данных, т.е. $t_{пер}=V/R$. При передаче пакетов произвольного объёма $t_{пер}$ является случайной величиной, распределенной по закону $B(t)$. В случае нарушения работоспособности сеть восстанавливается за случайное время $t_{в_i}$; $i=\overline{1,n}$ с ФР времени восстановления $\Delta_i(t)$, а поступивший пакет данных передается повторно.

Входящий поток пакетов данных является редкоследующим, а КА возможны как во время передачи пакетов, так и в паузах между ними. Количество мест для ожидания передачи считается неограниченным.

Требуется определить математическое ожидание $\overline{T}_h$ и функцию распределения $F(t)$ времени успешной передачи пакетов данных в условиях КА, реализуемых нарушителем.

Решение:

Представим процесс функционирования сети -IP при реализации нарушителем двух видов КА в виде стохастической сети (рис.2.12). Предположим, что $\Delta_1(t)=1-e^{\delta_1 t}$; $\Delta_2(t)=1-e^{\delta_2 t}$; $\beta(t)=1-e^{\beta t}$.

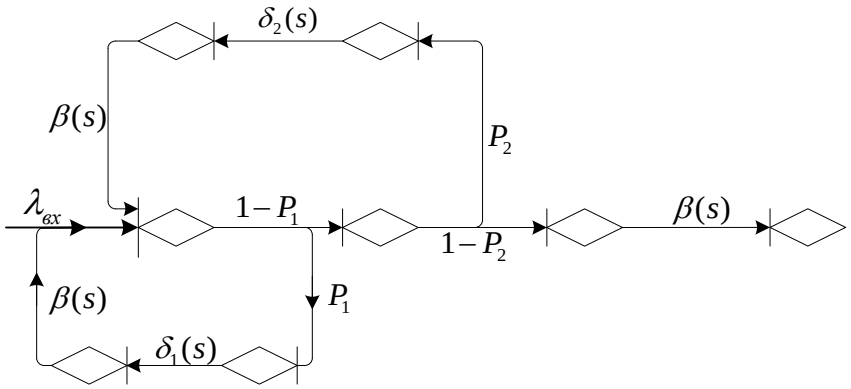

Рисунок 2.12 – Стохастическая сеть процесса функционирования сети IP при реализации нарушителем двух видов КА

Используя уравнение Мейсона для замкнутых графов, составим эквивалентную функцию стохастической сети:

$$h(s)=\frac{(1-P_1)(1-P_2)\beta(s)k\left(\overline{d}+s+\overline{c}\right)}{\left[1-P_1\delta_1(s)\beta(s)-P_2\delta_2(s)\beta(s)(1-P_1)\right]\left(\overline{d}+s\right)}, \qquad (2.38)$$

где $h_0=\frac{b(P_1-1)(P_2-1)\left(\overline{c}+\overline{d}\right)}{\overline{d}\left(P_1+P_2-P_1P_2-b\right)}$; $\overline{d}=d_1P_1+d_2P_2$; $\overline{c}=\frac{P_1}{t_{рв1}}+\frac{P_2}{t_{рв2}}$; $k=\frac{\overline{d}}{\overline{d}+\overline{c}}$; $d_1=\frac{1}{t_{в1}}$;

$d_2=\frac{1}{t_{в2}}$; $b=\frac{1}{t_n}$.

Представим знаменатель эквивалентной функции в каноническом виде, то есть это позволяет перейти к разложению Хевисайда для случая простых полюсов [6-13, 31, 48]:

$$h(s)=\sum_{i=1}^{4}\frac{\left(\overline{d}+\overline{c}+s\right)\left(d_1+s\right)\left(d_2+s\right)\left(1-P_1\right)\left(1-P_2\right)bk}{4\left(s_i\right)^3+3\left(s_i\right)^2\cdot A+2s_i\cdot B+C},\qquad(2.39)$$

где $A=b+\overline{d}+d_1+d_2$; $B=b\overline{d}-P_2d_2-P_1d_1+bd_1+bd_2+\overline{d}d_1+\overline{d}d_2+d_1d_2+P_1P_2d_2$;

$C=b\overline{d}d_1-P_2\overline{d}d_2-P_1d_1d_2-P_2d_1d_2-P_1\overline{d}d_1+b\overline{d}d_2+bd_1d_2+\overline{d}d_1d_2+P_1P_2\overline{d}d_2+P_1P_2d_1d_2$.

Среднее время $\overline{T}_h$ успешной передачи пакетов равно (2.40):

$$\overline{T}_h=\frac{k\left(P_1-1\right)\left(P_2-1\right)[\overline{d}^2d_1d_2-P_2^2b\overline{d}^2d_1+b\overline{c}d_1d_2+\overline{c}\overline{d}d_1d_2+P_1b\overline{d}^2d_2+P_2b\overline{d}^2d_1-}{b\overline{d}^2d_1d_2\left(P_2-P_2^2+P_1-1\right)^2\cdot}$$
$$\frac{-P_2^2b\overline{c}\overline{d}d_1+P_2^2b\overline{c}d_1d_2+P_1b\overline{c}\overline{d}d_2+P_2b\overline{c}\overline{d}d_1-P_1b\overline{c}d_1d_2-P_2b\overline{c}d_1d_2]}{\cdot h(0)}\qquad(2.40)$$

Функция плотности распределения вероятностей времени передачи (2.41):

$$h(t)=\sum_{i=0}^{3}\frac{\left[\left(\overline{d}+s_i+\overline{c}\right)\left(d_1+s_i\right)\left(d_2+s_i\right)\left(1-P_2\right)bk\right]\cdot e^{s_it}}{\left[4\left(s_i\right)^3+3\left(s_i\right)^2\cdot A+2s_i\cdot B+C\right]\left(-s_i\right)h_0k},\qquad(2.41)$$

а интегральная функция плотности распределения вероятностей времени передачи (2.42):

$$H(t)=\sum_{i=0}^{3}\frac{\left[\left(\overline{d}+s_i+\overline{c}\right)\left(d_1+s_i\right)\left(d_2+s_i\right)\left(1-P_2\right)bk\right]\cdot\left(1-e^{s_it}\right)}{\left[4\left(s_i\right)^3+3\left(s_i\right)^2\cdot A+2s_i\cdot B+C\right]\left(-s_i\right)h_0\left(s_i\right)-s_k}.\qquad(2.42)$$

По формулам (2.39–2.42) были произведены расчеты, результаты которых представлены в виде семейства функций распределения на рис.2.13.

В ходе расчетов предполагалось, что:

- среднее время передачи пакета данных с объемом $V=10$ Мбит между соответствующими узлами равно 1с;

- среднее время восстановления работоспособности сети IP после успешной реализации нарушителем КА изменяется в пределах $t_{в_1}=3...5$ с и $t_{в_2}=2,5...4$ с соответственно;

- среднее время реализации нарушителем КА равно $t_{рв_1} = 50$ с и $t_{рв_2} = 100$ с соответственно;

- вероятность успешной реализации нарушителем КА принимает значения в диапазоне 0,08–0,8.

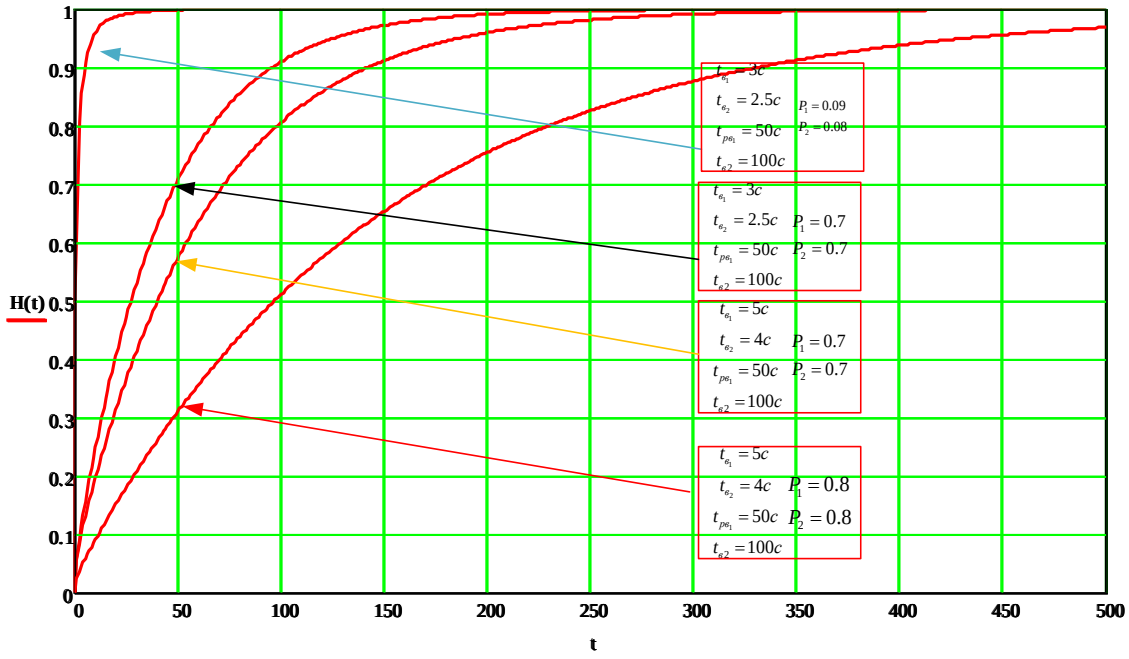

Рисунок 2.13 – Семейство функций распределения времени передачи пакетов в сети IP при осуществлении двух видов КА

В условиях осуществлении КА существенно растает роль эффективности механизма организации информационной безопасностью сети на базе IP-технологий, характеризующим в модели временем работоспособности после КА. Так, например, при вероятности успешной реализации нарушителем КА $P_i = 0,5$ незначительное увеличение времени восстановления работоспособности приводит к резкому увеличению среднего времени передачи пакетов [6-13, 31, 48]:

– время успешной передачи информации в сети зависит от способности нарушителя оказать КА на сетевые элементы. Так, например, если нарушитель способен успешно реализовать воздействие с вероятностью не хуже $P_i = 0,7$, то следует ожидать увеличения среднего времени доведения информации в сети более чем в пять раз;

– закон распределения времени успешной передачи пакета в общем случае является гиперэкспоненциальным и, как показано в [31, 48], может быть с достаточной точностью аппроксимирован неполной Гамма-функцией. Расчеты показывают, что полученное распределение обладает значительной правосторонней асимметрией (коэффициент асимметрии $K_A \geq 1,9$), является несущественно островершинным (коэффициент эксцесса $E_A \geq 5,7$), а поток успешно переданных пакетов является неоднородным (коэффициент вариации $K_B \geq 1,3$) [31, 48]. Следует ожидать, что параметр потока успешно переданных пакетов $\lambda(t) = \frac{f(t)}{1-F(t)}$ является непостоянным во времени и при $t \to \infty$ (2.43):

$$\lim_{t\to\infty} \lambda(t) = \lim_{t\to\infty} \frac{\sum_{k=1}^{n} \frac{V(s_k)}{U'(s_k)} e^{s_k t}}{1-(\sum_{k=1}^{n} \frac{V(s_k)}{U'(s_k)} S_k^{-1}(1-e^{s_k t}))} = \frac{\sum_{k=1}^{n} \frac{V(s_k)}{U'(s_k)} e^{s_k t} \cdot s_k}{\sum_{k=1}^{n} \frac{V(s_k)}{U'(s_k)} e^{s_k t}} \leq \frac{1}{T_h}; \qquad (2.43)$$

то есть интенсивность успешной передачи пакетов не превосходит интенсивности, определяемой как величина, обратная среднему времени успешной передачи пакетов $\frac{1}{T_h}$. Это говорит о том, что поток успешно переданных пакетов не является простейшим, в связи с чем актуализируется задача оценить время доведения информации в сетях -IP для случая, когда входящий поток не является редкоследующим, а соответствует реальному взаимодействию корреспондирующих пар в сети.

Таким образом, разработанная модель обеспечивает получение не противоречащих логике результатов, чувствительна к изменениям входных параметров и работоспособна.

Математическая модель процесса функционирования сети IP в условиях информационных воздействий при передаче самоподобного потока данных.

Постановка задачи: Пусть имеется сеть IP, в которой передаются пакеты данных. На этапе организации и планирования обмена информацией определяются маршруты передачи, каждый из которых в общем случае состоит из m узлов и $m-1$ участков. По маршруту передается поток категорированных пакетов, которые поступают в буфер памяти объемом $0 < E < \infty$. В зависимости от класса обслуживания (Quality of Service – QoS), пакетам присваиваются относительные приоритеты $i = \overline{1, R}$. Суммарная интенсивность поступления пакетов равна $\Lambda = \sum_{r=1}^{R} \lambda_r$, где λ_r–интенсивность потока пакетов*r*-го приоритета.

Сеть -IP функционирует в условиях КА нарушителя, каждая из которых нарушает работоспособность сетевых элементов с вероятностью P_i; $i = \overline{1, n}$. Если работоспособность сети не нарушена, то с вероятностью $1 - P_i$ подлежащие передаче пакеты *r*-го приоритета будут успешно переданы корреспонденту за случайное время $t_{пер,r}$, определяемое случайным объемом V_r и скоростью передачи R, равное $t_{пер,r} = \sum_{r=1}^{n-1} \frac{1}{\mu_r}$, где $\mu_r = R / V_r$ – интенсивность обслуживания пакета*r*-го приоритета, и характеризуемое функцией распределения (ФР) $B_r(t)$ -го.

В случае нарушения работоспособности -IP сеть восстанавливается за случайное время $t_{в_i}$; $i = \overline{1, n}$ с ФР времени восстановления $\Delta_i(t)$, а поступивший пакет данных передается повторно.

Входящий поток пакетов характеризуется распределениями Вейбулла или Паретто. Деструктивные воздействия на сетевые элементы возможны как во время передачи пакетов, так и в паузах между ними. Количество мест для ожидания определяется емкостью накопителя [16-13, 31, 48].

Требуется определить математическое ожидание времени передачи пакета между соответствующими узлами $\overline{T_h}$ и функцию распределения времени успешной передачи пакетов данных в условиях КА.

Решение:

Представим описанный выше процесс в виде стохастической сети (рис. 2.14).

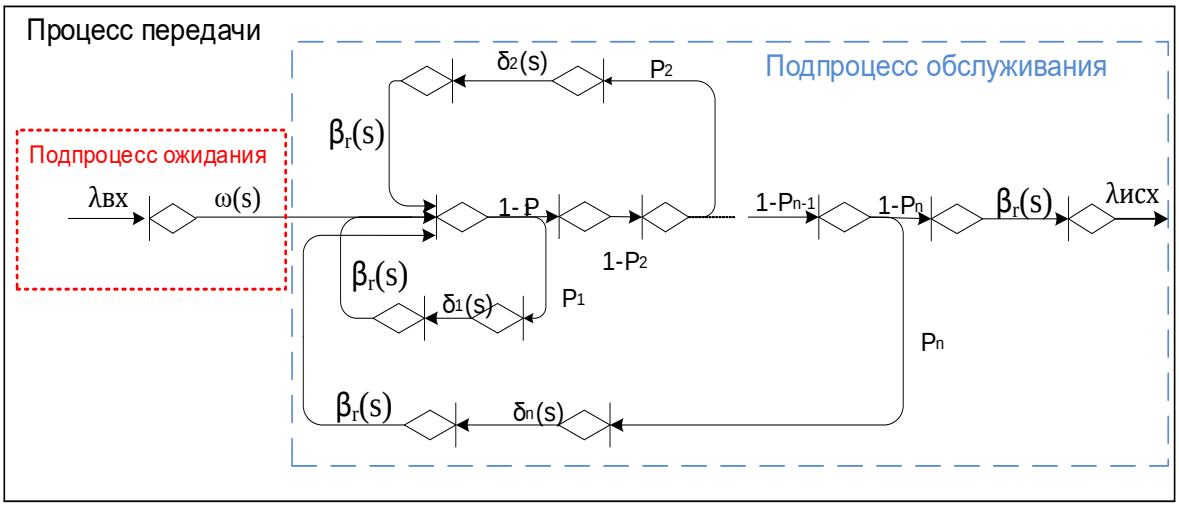

Рисунок 2.14 – Стохастическая сеть процесса передачи

Условно процесс передачи разделен на подпроцесс ожидания и подпроцесс непосредственно передачи (обслуживания). Подпроцесс ожидания в очереди на передачу характеризуется случайным временем ожидания $t_{ож}$ с ФР времени ожидания $\omega(t)$. Процесс обслуживания характеризуется средним временем передачи пакета $\overline{t_{h_r}}$ между соответствующими узлами с ФР времени обслуживания $\mu_r(t)$.

В стохастической сети обозначены:

$\beta_r(s) = \int_0^\infty e^{-st} d[B_r(t)]$ – преобразование Лапласа–Стилтьеса, то есть функция распределения времени передачи пакетов *r*-й категории срочности без учета КА нарушителя;

$P_1,...,P_n$ – вероятность воздействия нарушителя КА;

$\delta_i(s) = \int_0^{\infty} e^{-st} d[\Delta_i(t)]$, $i = \overline{1,n}$ – преобразование Лапласа–Стилтьеса, то есть функция распределения времени восстановления сети после *i*-й КА;

$\lambda_{вх}$, $\lambda_{исх}$ – интенсивность входящего и исходящего потоков пакетов;

$\omega_r(s) = \int_0^{\infty} e^{-st} d[W_r(t)]$ – преобразование Лапласа–Стилтьеса, то есть функция распределения времени ожидания передачи сообщений *r*-й категории срочности.

Функция распределения времени передачи подпроцесса обслуживания получена в работах авторов [3, 15, 23, 53-55] и имеет вид (2.44):

$$H_r(t) = \sum_{i=1}^{n} \frac{V(s_{ir}) \cdot \left(1 - e^{s_{ir} t}\right)}{U'(s_{ir}) \cdot \left(-s_{ir}\right)}, \tag{2.44}$$

где

$V(s_{ir}) = k\beta(s_{ir})\left(\overline{d} + \overline{c} + s_{ir}\right)\prod_{i=1}^{n}(1 - P_i)$;

$$U'(s_{ir}) = \overline{d}\left[1 - \beta(s_{ir})\sum_{i=1}^{n} P_i \delta_i(s_{ir}) \prod_{j=1}^{i-1}\left(1 - P_j\right)\right] + \left(\overline{d} + s_{ir}\right) \cdot$$
$$\cdot \left[-\beta'(s_{ir})\sum_{i=1}^{n} P_i \delta_i(s_{ir}) \prod_{j=1}^{i-1}\left(1 - P_j\right) - \beta(s_{ir})\sum_{i=1}^{n} P_i \delta_i'(s_{ir}) \prod_{j=1}^{i-1}\left(1 - P_j\right)\right].$$

$\overline{d} = \sum_{i=1}^{n} t_{ei}^{-1} P_i$ – математическое ожидание интенсивности восстановления сетевого элемента после КА;

$\overline{c} = \sum_{i=1}^{n} t_{pei}^{-1} P_i$ – математическое ожидание интенсивности реализации нарушителем КА на сеть;

$k = \frac{\overline{d}}{\overline{d} + \overline{c}}$ – вероятность восстановления работоспособности сетевых элементов за время повторной передачи пакета и реализации очередной КА.

Знание функции распределения позволяет определить математическое ожидание и дисперсию (2.45-2.46):

$$\overline{T}_r = \int_0^{\infty} td\left[H_r(t)\right] = \sum_{i=1}^{n} \frac{V(s_{ir})}{U'(s_{ir})(s_{ir})^2}; \tag{2.45}$$

$$D_r = \int_0^{\infty} (t-T)^2 d\left[H_r(t)\right] = \sum_{i=1}^{n} \frac{2V(s_{ir})}{U'(s_{ir})(s_{ir})^3} - T^2 \tag{2.46}$$

и коэффициент вариации времени обслуживания (2.47):

$$C_{hr} = \frac{\sqrt{D_r}}{T_r} \tag{2.47}$$

В работе [6-13, 31, 48] было показано, что ФР может быть аппроксимирована неполной Гамма-функцией, то есть (2.48):

$$H_r(t) \approx F_{\gamma r}(t) = \frac{m_r^{\alpha_r}}{\Gamma(\alpha_r)} \int_0^t t^{\alpha_r - 1} \cdot \exp(-m_r t) dt, \tag{2.48}$$

где

$m_r = \frac{T_h}{D_h}; \alpha_r = \frac{T_h^{\,2}}{D_h}$ – параметр масштаба и формы неполной Гамма-функции.

Погрешность такой аппроксимации не превышает 10%, что иллюстрирует рис. 2.15.

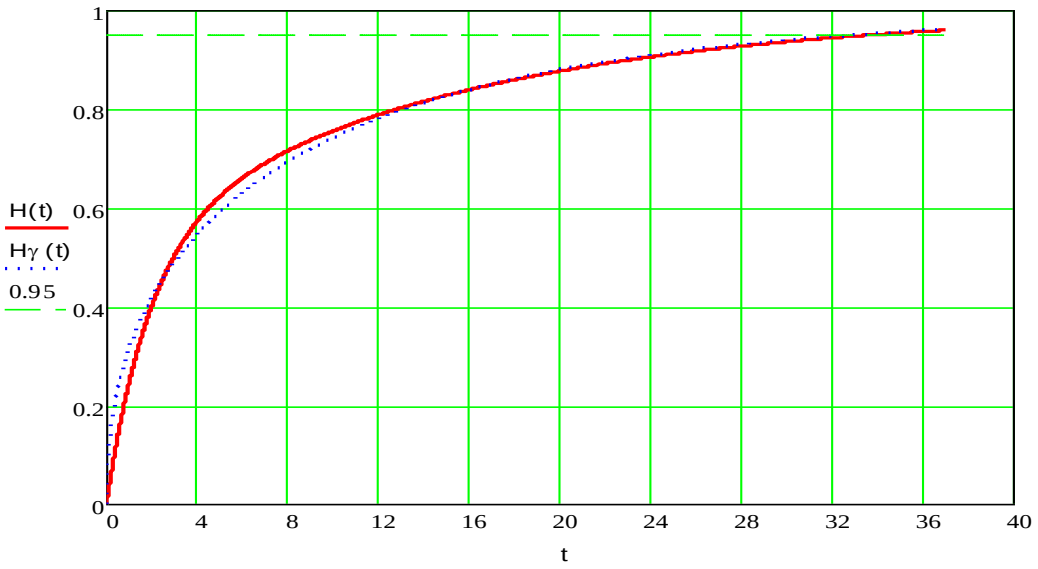

Рисунок 2.15 –Аппроксимация ФР времени передачи неполной Гамма-функцией

Таким образом, с точностью, достаточной для инженерных расчётов, изображение ФР $H_r(t)$ по Лапласу–Стилтьесу может быть определенно как изображение неполной Гамма-функции, т.е.

$$h_{\gamma_r}(s) = \left(\frac{m_r}{m_r + s} \right)^{\alpha_r} \tag{2.49}$$

Это позволяет представить процесс передачи пакетов в виде укрупненной стохастической сети (рис. 2.16) с эквивалентной функцией *Q(s)*:

$Q_r(s) = \omega_r(s) h_{\gamma r}(s)$.

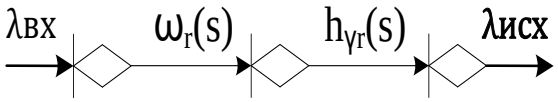

Рисунок 2.16 – Укрупненная стохастическая сеть процесса передачи

При определении $\omega_r(s)$ будем исходить из следующих известных утверждений:

– система массового обслуживания (СМО) с конечным и бесконечным буфером при малых нормах потерь пакетов (менее 10^{-3}) обладает свойством эквивалентности [6-13, 31, 48];

– на основании «закона сохранения накопленной в очереди работы» накопленная в очереди с приоритетами работа постоянна и равна накопленной работе в бесприоритетной СМО с суммарной нагрузкой;

– длина очереди на обслуживание (на передачу), а значит, и время ожидания в очереди не зависят от законов распределения времени между поступлением пакетов и времени обслуживания, а определяются только первыми двумя моментами [31, 48].

Исходя из результатов [31, 48] получены выражения для определения:

– первого момента, т.е. среднего времени ожидания обслуживания пакетов *r*-го приоритета (2.50):

$$\overline{T_{\omega r}} = \begin{cases} \overline{T}^{*}_{\omega r}, r = 1; \\ \frac{\Lambda_r}{\lambda_r}\left(\overline{T}^{*}_{\omega r} - \frac{\Lambda_{r-1}}{\Lambda_r}\overline{T}^{*}_{\omega r-1}\right), r = \overline{2,R} \end{cases}, \quad (2.50)$$

где среднее время ожидания обслуживания пакетов без приоритетов с учетом изменчивости распределений времени между поступлениями пакетов и времени обслуживания

$$\overline{T}^{*}_{\omega r} = \frac{\rho_r - \rho_r^{K+2}}{1-\rho_r^{K+2}} \frac{1-(K+1)\rho_r^{K} + K\rho_r^{K+1}}{\mu_r(1-\rho_r)(1-\rho_r^{K+1})} \frac{C_\omega + C_{hr}}{2};$$

$\rho_r = \lambda_r \overline{T_r}; \overline{T_r}$ – математическое ожидание времени передачи пакетов в условиях КА при редкоследующем входном потоке (2.50).

В свою очередь, дисперсия времени ожидания равна (2.51):

$$D_\omega = \begin{cases} M_{2\omega r} - \left(\overline{T_r}\right)^2, r = 1; \\ \left(\left(\frac{\lambda_i}{\Lambda}\right)^3 \left[M_{2\omega r} - \sum_{i=1}^{r-1}\left(\frac{\lambda_i}{\Lambda}\right)^3 M_{2\omega r-1}\right]\right) - \left(\overline{T_r}\right)^2 r = \overline{2,R} \end{cases}, \quad (2.51)$$

где:

– второй момент времени ожидания без учета приоритетов

$$M_{2\omega r-1} = \left(\frac{C_\omega^{\,2} + C_{hr}^{\,2}}{2}\right)^2 \times \frac{\rho_r - \rho_R^{K+2}}{1-\rho_R^{K+2}} \times$$
$$\times \frac{2(1-\rho_r^{K}) + K\rho_r^{K}(1-\rho_r)\left[\rho_r(K+1) - K - 3\right]}{(1-\rho_r)^2(1-\rho_r^{K+1})} \times \sum_{i=1}^{n} \frac{2V(s_{ir})}{U'(s_{ir})(s_{ir})^2},$$

– коэффициент вариации времени между поступлениями пакетов $C_{\omega r}$ и времени обслуживания (передачи) пакетов C_{hr}.

В отличие от [31] предлагается аппроксимировать ФР времени ожидания неполной Гамма-функцией, что хорошо согласуется с результатами, опубликованными в [6-13, 31, 48]. Поэтому изображение ФР по Лапласу–Стилтьесу (2.52):

$$\omega_r(s) = \begin{cases} \left(\frac{\omega_r}{\omega_r + s}\right)^{\beta_r} \\ \frac{\Lambda_r}{\lambda_r}\left(\left(\frac{\omega_r}{\omega_r + s}\right) - \frac{\Lambda_{r-1}}{\Lambda_r}\left(\frac{\omega_r}{\omega_{r-1} + s}\right)^{\beta_{r-1}}\right) r = \overline{2,R} \end{cases}, \quad (2.52)$$

где

$\omega_r = \frac{\overline{T_{\omega r}}}{D_\omega}$; $\beta_r = \frac{\left(\overline{T_{\omega r}}\right)^2}{D_\omega}$ – параметр масштаба и формы Гамма-распределения [31, 48].

Таким образом, эквивалентная функция стохастической сети (см. рис. 2.16) примет вид (2.53):

$$Q_r(s) = \begin{cases} \left(\frac{\omega_r}{\omega_r + s}\right)^{\beta_r} \left(\frac{m_r}{m_r + s}\right)^{\alpha_r}, \; r = 1, \\ \frac{\Lambda_r}{\lambda_r}\left(\left(\frac{\omega_r}{\omega_r + s}\right)^{\beta_r} \left(\frac{m_r}{m_r + s}\right)^{\alpha_r} - \frac{\Lambda_{r-1}}{\Lambda_r}\left(\frac{\omega_{r-1}}{\omega_{r-1} + s}\right)^{\beta_{r-1}} \left(\frac{m_{r-1}}{m_{r-1} + s}\right)^{\alpha_{r-1}}\right), \; r = \overline{2, R}, \end{cases}, \quad (2.53)$$

а ФР времени задержки (процесса передачи) ф.2.54.

$$F_r(t) = \begin{cases} F_r(t), \; r = 1, \\ \frac{\Lambda_r}{\lambda_r}\left(F_r(t) - \frac{\Lambda_{r-1}}{\Lambda_r} F_{r-1}(t)\right) r = \overline{2, R}, \end{cases} \quad (2.54)$$

где:

$F_r(t) = \frac{\chi^{\varepsilon_r}}{\Gamma(\varepsilon_r)} \int_0^t x^{\varepsilon_{r-1}} \exp(-x\chi_r) dx$;

$\chi_r = \frac{T_{\omega r} + \overline{T_r}}{D_{\omega r} + D_r}$; $\varepsilon_r = \frac{\left(T_{\omega r} + \overline{T_r}\right)^2}{D_{\omega r} + D_r}$.

Вероятность потери пакетов различных приоритетов равна (2.55):

$$P_{K+1} = \frac{\rho - \rho^{K/C^2+2}}{1 - \rho^{K/C^2+2}} \frac{1 - \rho}{1 - \rho^{K/C^2+1}} \rho^{K/C^2}. \quad (2.55)$$

Для установления ФР времени задержки необходимо определить коэффициент вариации входящего потока $C_{\omega r}$, который существенно зависит от вида модели распределения длительности интервалов времени между пакетами во входящем потоке Парето (2.56):

$$C_{\omega П}{}^2 = \left(\frac{\phi^2{}_{\max_r} \phi^{\alpha_r}{}_{\min_r} - \phi^{\alpha_r}{}_{\max_r} \phi^2{}_{\min_r}}{2-\alpha_r} - \frac{\alpha_r \left(\phi_{\max_r} \phi^{\alpha_r}{}_{\min_r} - \phi^{\alpha_r}{}_{\max_r} \phi_{\min_r} \right)^2}{(1-\alpha_r)^2 \left(\phi^{\alpha_r}{}_{\max_r} - \phi^{\alpha_r}{}_{\min_r} \right)} \right) \times ,$$

$$\times \frac{(1-\alpha_r)^2 \left(\phi^{\alpha_r}{}_{\max_r} - \phi^{\alpha_r}{}_{\min_r} \right)}{\alpha_r \left(\phi_{\max_r} \phi^{\alpha_r}{}_{\min_r} - \phi^{\alpha_r}{}_{\max_r} \phi_{\min_r} \right)^2} \qquad (2.56)$$

а при распределении Вейбула (2.57):

$$C_{\omega B} = \sqrt{\frac{\Gamma\left(1+\frac{2}{\alpha_r}\right)}{\Gamma^2\left(1+\frac{1}{\alpha_r}\right)} - 1}, \qquad (2.57)$$

где: Г(*)– Гамма-функция.

Входящий поток, который в общем случае является самоподобным, характеризуется H-коэффициентом Херста. Выражения для расчета коэффициента H существенно зависит от параметра α_r–формы распределения Вейбула или Парето. По результатам имитационного моделирования в [31] была получена эмпирическая формула для расчета коэффициента Херста Hw: при распределении Вейбула коэффициент Херста определяется выражением $Hw = 1.2\exp(-9\alpha_r) + 0.51$, где α_r – параметр распределения Вейбула, численно равный [31, 48]:

$$\alpha_r = \begin{cases} 3 - 2Hw, при\ 0 \le Hw \le 0,51; \\ -\frac{1}{9} Ln \frac{Hw - 0.51}{1.2}, при\ 0,51 \prec Hw \le 0,6; \\ -\frac{1}{19} Ln \frac{Hw1 - 0.57}{4.1} при\ 0,6 \le Hw \le 1; \end{cases};$$

– при распределении Парето параметр α_r определяется выражением [48] $\alpha_r = H^{-(1/0,8)}$.

Таким образом, все искомые величины, необходимые для расчета функции распределения, установлены. Для демонстрации работоспособности модели рассмотрим следующую постановку задачи.

Постановка частной задачи: Пусть имеется сеть IP, в которой передаются пакеты данных. На этапе организации и планирования информационного обмена определяются маршруты передачи, каждый из которых, в общем, случае состоит из n узлов, и $n-1$ участков. По маршруту передается поток категорированных пакетов, которые поступают в буфер памяти объемом $0 < E < \infty$. В зависимости от класса обслуживания Quality of Service (QoS), пакетам присваиваются относительные приоритеты $r = \overline{1,R}$. Суммарная интенсивность поступления пакетов равна $\Lambda = \sum_{r=1}^{R} \lambda_r$, где λ_r – интенсивность потока пакетов *r*-го приоритета.

Сеть -IP функционирует в условиях КА нарушителя, каждая из которых нарушает работоспособность сетевых элементов с вероятностью $P_i; i = \overline{1,2}$. Если работоспособность сети не нарушена, то с вероятностью $(1-P_i)$ подлежащие передаче пакеты *r*-го приоритета будут успешно переданы корреспонденту за случайное время $t_{пер_r}$,определяемое случайным объемом V_r и скоростью передачи R, равное $t_{пер_r} = \sum_{r=1}^{n-1} \frac{1}{\mu_r}$, где $\mu_r = R / V_r$ – интенсивность обслуживания пакета *r*-го приоритета, характеризуемое функцией распределения (ФР) $B_r(t)$.

В случае нарушения работоспособности сеть -IP восстанавливается за случайное время $t_{в_i}$, $i = \overline{1,2}$ с ФР $\Delta_i(t)$, а поступивший пакет данных передается повторно.

Входящий поток пакетов характеризуется распределениями Вейбула или Паретто. Деструктивные воздействия на сетевые элементы сети возможны как во время передачи пакетов, так и в паузах между ними. Количество мест для ожидания определяется емкостью накопителя.

Требуется определить математическое ожидание времени передачи пакета между соответствующим узлами ($\overline{T_{\Sigma r}}$) и функцию распределения времени успешной передачи пакетов данных в условиях КА.

Решение: Представим описанный процесс в виде укрупненной стохастической сети (рис.2.7), в которой $h_{\gamma r}(s)$ определяется формулой

$$h_{\gamma_r}(s) = \left(\frac{m_r}{m_r + s}\right)^{\alpha_r},$$

где $m_r = \frac{T_r}{D_r}; \alpha_r = \frac{T_r^2}{D_r}$ – параметры масштаба и формы неполной Гамма-функции соответственно; $T_r = \sum_{i=1}^{4} \frac{(\bar{d} + \bar{c} + s)(d_1 + s)(d_2 + s)(1 - P_1)(1 - P_2) b_r k}{(4(s_1)^3 + 3(s_1)^2 \cdot A_r + 2s_1 B_r + C_r) s_i^2}$ – среднее время обслуживания (непосредственно передачи) пакета, (2.58); $D_r = \sum_{i=1}^{4} \frac{2(\bar{d} + \bar{c} + s)(d_1 + s)(d_2 + s)(1 - P_1)(1 - P_2) b_r k}{(4(s_1)^3 + 3(s_1)^2 \cdot A_r + 2s_1 B_r + C_r) s_i^3} - T_r^2$ – дисперсия времени обслуживания (непосредственно передачи) пакета (рис.2.17).

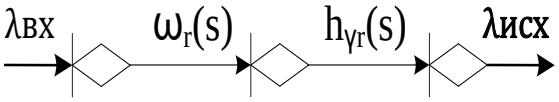

Рисунок 2.17 – Укрупненная стохастическая сеть процесса передачи

В свою очередь, преобразование ЛС ФР времени ожидания передачи определим как

$$\omega_r(s) = \begin{cases} \left(\frac{\omega_r}{\omega_r + s}\right)^{\beta_r}, r = 1 \\ \frac{\Lambda_r}{\lambda_r}\left(\left(\frac{\omega_r}{\omega_r + s}\right) - \frac{\Lambda_{r-1}}{\Lambda_r}\left(\frac{\omega_r}{\omega_{r-1} + s}\right)^{\beta_{r-1}}\right); r = \overline{2, R} \end{cases},$$

где $\omega_r = \frac{\overline{T_{\omega r}}}{D_\omega}$; $\beta_r = \frac{\left(\overline{T_{\omega r}}\right)^2}{D_\omega}$ – параметр масштаба и формы Гамма-распределения;

$$\overline{T_{\omega r}} = \begin{cases} \overline{T}^{*}_{\omega r}, r = 1; \\ \frac{\Lambda_r}{\lambda_r}\left(\overline{T}^{*}_{\omega r} - \frac{\Lambda_{r-1}}{\Lambda_r}\overline{T}^{*}_{\omega r-1}\right), r = \overline{2,R} \end{cases}$$ – среднее время ожидания передачи;

$$D_{\omega} = \begin{cases} M_{2\omega r} - \left(\overline{T_r}\right)^2, r = 1; \\ \left(\left(\frac{\lambda_i}{\Lambda}\right)^3\left[M_{2\omega r} - \sum_{i=1}^{r-1}\left(\frac{\lambda_i}{\Lambda}\right)^3 M_{2\omega r-1}\right]\right) - \left(\overline{T_r}\right)^2 r = \overline{2,R} \end{cases}$$ – дисперсия времени ожидания передачи.

здесь эквивалентная функция стохастической сети (см. рис.2.17) равна

$$Q_r(s) = \begin{cases} \left(\frac{\omega_r}{\omega_r + s}\right)^{\beta_r}\left(\frac{m_r}{m_r + s}\right)^{\alpha_r}, r = 1, \\ \frac{\Lambda_r}{\lambda_r}\left(\left(\frac{\omega_r}{\omega_r + s}\right)^{\beta_r}\left(\frac{m_r}{m_r + s}\right)^{\alpha_r} - \frac{\Lambda_{r-1}}{\Lambda_r}\left(\frac{\omega_{r-1}}{\omega_{r-1} + s}\right)^{\beta_{r-1}}\left(\frac{m_{r-1}}{m_{r-1} + s}\right)^{\alpha_{r-1}}\right), r = \overline{2,R}, \end{cases},$$

а функция распределения с учетом (2.54), имеет вид:

$$F_r(t) = \begin{cases} F_r(t), r = 1, \\ \frac{\Lambda_r}{\lambda_r}\left(F_r(t) - \frac{\Lambda_{r-1}}{\Lambda_r}F_{r-1}(t)\right) r = \overline{2,R} \end{cases}, \quad (2.59)$$

где

$$F_r(t) = \frac{\chi^{\varepsilon_r}}{\Gamma(\varepsilon_r)}\int_0^t x^{\varepsilon_{r-1}}\exp(-x\chi_r)dx;$$

$$\chi_r = \frac{T_{\omega r} + \overline{T_r}}{D_{\omega r} + D_r};\ \varepsilon_r = \frac{\left(T_{\omega r} + \overline{T_r}\right)^2}{D_{\omega r} + D_r}.$$

По формуле (2.59) произведены расчеты, результаты которых представлены на рис. 2.18. При расчетах использовались следующие исходные данные. Интенсивность суммарного потока 40 пакетов в секунду, при этом поток описывается моделью Вейбула с индексом Херста H=0,91; коэффициенты масштаба и формы распределения Вейбула 1,1 и 5 соответственно; число участков передачи на маршруте – 10; скорость передачи пакетов 150 Мбит/с; среднее время восстановления работоспособности сетевых элементов после КА – 2 с; вероятность успешной

реализации нарушителем КА P_1=P_2= 0,00001–0,1, при времени успешной реализации КА 200…300с; объем накопителя сетевого элемента – 20 пакетов, каждый из которых имеет объем 48 байт.

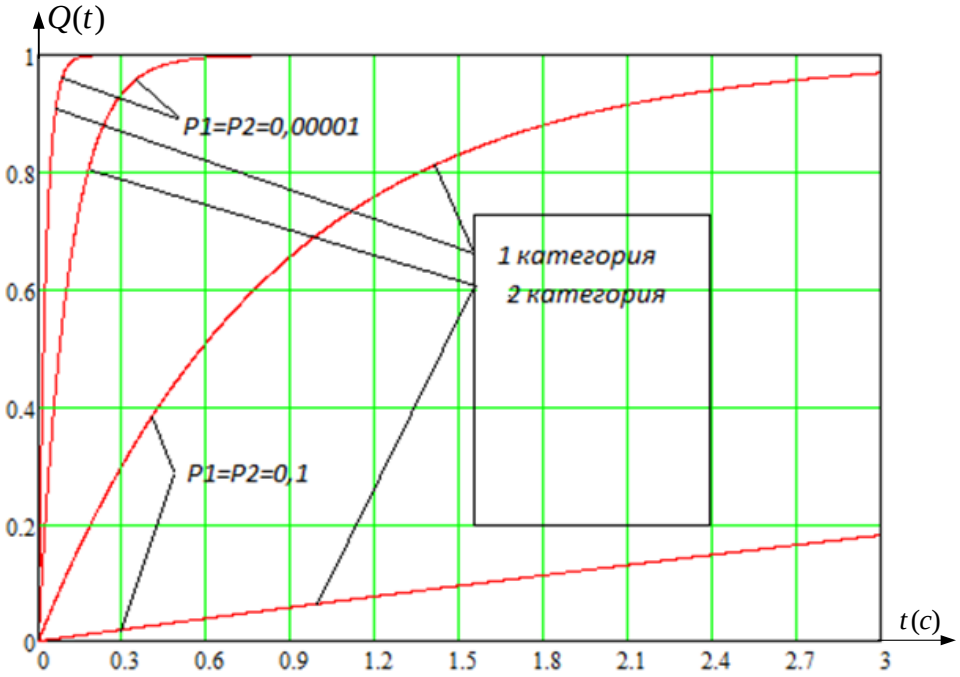

Рисунок 2.18 – Семейство функций распределения времени успешной передачи пакетов при $\lambda_1 = 10\,пак./c$; $\lambda_2 = 30\,пак./c$ и различных значениях вероятности успешной реализации нарушителем КА

Расчеты показывают, что в случае существенно затрудненных КА вероятность потери пакетов 1-й категории составляет $5{,}1 \cdot 10^{-4}$, пакетов 2-й категории – 0,056, при этом среднее время успешной передачи пакетов 1-й категории составляет 0,028с, пакетов 2-й категории 0,25с, джиттер задержки пакетов обоих категорий не превышает 0,076с. Когда нарушитель может успешно реализовать КА с вероятностью не хуже 0,1, среднее время успешной передачи для пакетов 1-й категории увеличивается до 0,9 с, вероятность потери пакетов – до 0,089, а джиттер– до 0,852с.

ГЛАВА 3. МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В БАНКОВСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

3.1. Криптографические способы защиты информации в БИС. Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях. Исторически криптография (в переводе с греческого этот термин означает «тайнопись») зародилась как способ скрытой передачи сообщений. Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы защитить эти данные, сделав их бесполезными для незаконных пользователей. Для обеспечения безопасности данных необходимо поддерживать три основные функции [27-29]:

– защиту конфиденциальности передаваемых или хранимых в памяти данных;

– подтверждение целостности и подлинности данных;

– аутентификацию абонентов при входе в систему и при установлении соединения.

Для реализации указанных функций используются криптографические технологии шифрования, цифровой подписи и аутентификации. Конфиденциальность обеспечивается с помощью алгоритмов и методов симметричного и асимметричного шифрования, а также путем взаимной аутентификации абонентов на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарткарт и т.п. Целостность и подлинность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на односторонних функциях и асимметричных методах шифрования. Аутентификация разрешает устанавливать соединения только между легальными пользователями и предотвращает доступ к средствам сети нежелательных лиц. Обеспечение конфиденциальности, целостности и подлинности, передаваемых и сохраняемых данных осуществляется, прежде всего, правильным

использованием криптографических способов и средств защиты информации. Основой большинства криптографических средств защиты информации является шифрование данных.

Под шифром понимают совокупность процедур и правил криптографических преобразований, используемых для зашифровывания и расшифровывания информации по ключу шифрования. **Под зашифровыванием информации** понимается процесс преобразования открытой информации (исходный текст) в зашифрованный текст (шифртекст). Процесс восстановления исходного текста по криптограмме с использованием ключа шифрования называют **расшифровыванием (дешифрованием)**.

Обобщенная схема криптосистемы шифрования показана на рис.3.1.

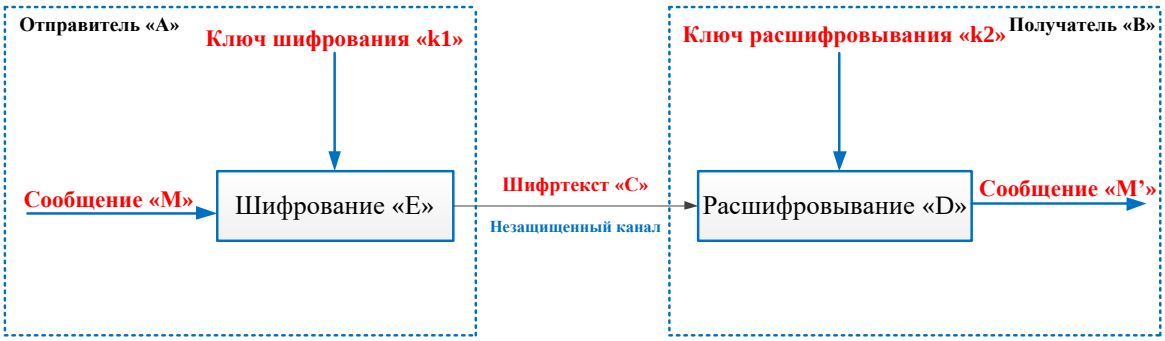

Рисунок 3.1 – Обобщенная схема криптосистемы шифрования

Исходный текст передаваемого сообщения (или хранимой информации) M зашифровывается с помощью криптографического преобразования E_{k1} с получением в результате шифртекста C (3.1):

$$C = E_{k1}(M) \tag{3.1}$$

где $k1$ – параметр функции E, называемый ключом шифрования.

Шифртекст C, называемый также криптограммой, содержит исходную информацию M в полном объеме, однако последовательность знаков в нем внешне представляется случайной и не позволяет восстановить исходную информацию без знания ключа шифрования $k1$. Ключ шифрования является

тем элементом, с помощью которого можно варьировать результат криптографического преобразования. Данный элемент может принадлежать конкретному пользователю или группе пользователей и являться для них уникальным. Зашифрованная с использованием конкретного ключа информация может быть расшифрована только его владельцем.

Обратное преобразование информации выглядит следующим образом (3.2):

$$M' = D_{k2}(C) \tag{3.2}$$

Функция D является обратной к функции E и производит расшифровывание шифртекста. Она также имеет дополнительный параметр в виде ключа $k2$. Ключ расшифровывание $k2$ должен однозначно соответствовать ключу $k1$, в этом случае полученное в результате расшифровывания сообщение M' будет эквивалентно M. При утствии верного ключа $k2$ получить исходное сообщение $M' = M$ с помощью функции D невозможно. Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифровывания. Соответственно различают два класса криптосистем:

- симметричные криптосистемы (с единым ключом);
- асимметричные криптосистемы (с двумя ключами).

Симметричные криптосистемы шифрования. Исторически первыми появились симметричные криптографические системы. В симметричной криптосистеме шифрования используется один и тот же ключ для зашифровывания и расшифровывания информации. Это означает, что любой, кто имеет доступ к ключу шифрования, может расшифровать сообщение. Соответственно с целью предотвращения несанкционированного раскрытия зашифрованной информации все ключи шифрования в симметричных криптосистемах должны держаться в секрете. Именно поэтому симметричные криптографические системы называют криптосистемами с секретным ключом – ключ шифрования должен быть доступен только тем,

кому предназначено сообщение. Симметричные криптосистемы называют еще одноключевыми криптографическими системами, или криптосистемами с закрытым ключом. Схема симметричной криптосистемы шифрования показана на рис.3.2.

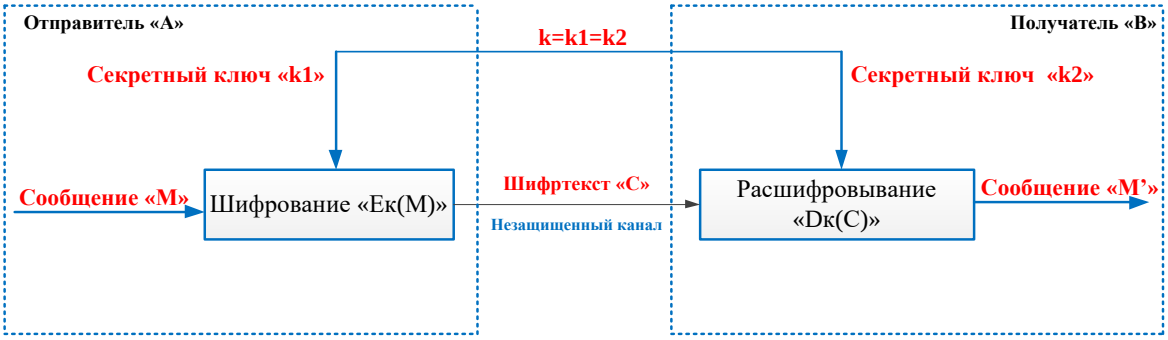

Рисунок 3.2 – Схема симметричной криптосистемы шифрования

Данные криптосистемы характеризуются наиболее высокой скоростью шифрования, и с их помощью обеспечиваются как конфиденциальность и подлинность, так и целостность передаваемой информации. Конфиденциальность передачи информации с помощью симметричной криптосистемы зависит от надежности шифра и обеспечения конфиденциальности ключа шифрования. Обычно ключ шифрования представляет собой файл или массив данных и хранится на персональном ключевом носителе (флэш-карта, диск, дискета). Подлинность обеспечивается за счет того, что без предварительно расшифровывания практически невозможно осуществить смысловую модификацию и подлог криптографически закрытого сообщения. Ложное сообщение не может быть правильно зашифровано без знания секретного ключа.

Целостность данных обеспечивается присоединением к передаваемым данным специального кода (имитовставки), вырабатываемой по секретному ключу. Имитовставка является разновидностью контрольной суммы, т.е. некоторой эталонной характеристикой сообщения, по которой осуществляется проверка целостности сообщения. Алгоритм формирования имитовставки должен обеспечивать ее зависимость по некоторому сложному

криптографическому закону от каждого бита сообщения. Проверка целостности сообщения выполняется получателем сообщения путем выработки по секретному ключу имитовставки, соответствующей полученному сообщению, и ее сравнения с полученным значением имитовставки. При совпадении делается вывод о том, что информация не была модифицирована на пути от отправителя к получателю.

Обладая высокой скоростью шифрования, одноключевые криптосистемы позволяют решать многие важные задачи защиты информации. Однако автономное использование симметричных криптосистем в компьютерных сетях порождает проблему распределения ключей шифрования между пользователями. Перед началом обмена зашифрованными данными необходимо обменяться секретными ключами со всеми адресатами. Передача секретного ключа симметричной криптосистемы не может быть осуществлена по общедоступным каналам связи, секретный ключ надо передавать отправителю и получателю по защищенному каналу. Для обеспечения эффективной защиты циркулирующих в сети сообщений необходимо огромное число часто меняющихся ключей (один ключ на каждую пару пользователей). При передаче ключей пользователям необходимо обеспечить конфиденциальность, подлинность и целостность ключей шифрования, что требует больших дополнительных затрат. Эти затраты связаны с необходимостью передачи секретных ключей по закрытым каналам связи или распределением таких ключей с помощью специальной службы доставки.

Проблема распределения секретных ключей при большом числе пользователей является весьма трудоемкой и сложной задачей. В сети на N пользователей необходимо распределить $\frac{N \cdot (N-1)}{2}$ секретных ключей, т.е. число распределяемых секретных ключей растет по квадратичному закону с увеличением числа абонентов сети.

Асимметричные криптосистемы шифрования. Асимметричные криптографические системы были разработаны в 1970-х гг. Принципиальное отличие асимметричные криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и ее последующего расшифровывания используются различные ключи:

- **открытый ключ** K используется для шифрования информации, вычисляется из секретного ключа k;
- **секретный ключ** k используется для расшифровывания информации, зашифрованной с помощью парного ему открытого ключа K.

Эти ключи различаются таким образом, что с помощью вычислений нельзя вывести секретный ключ k из открытого ключа K. Поэтому открытый ключ K может свободно передаваться по каналам связи. Асимметричные системы называют также двухключевыми криптографическими системами, или криптосистемами с открытым ключом. Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом показана на рис.3.3.

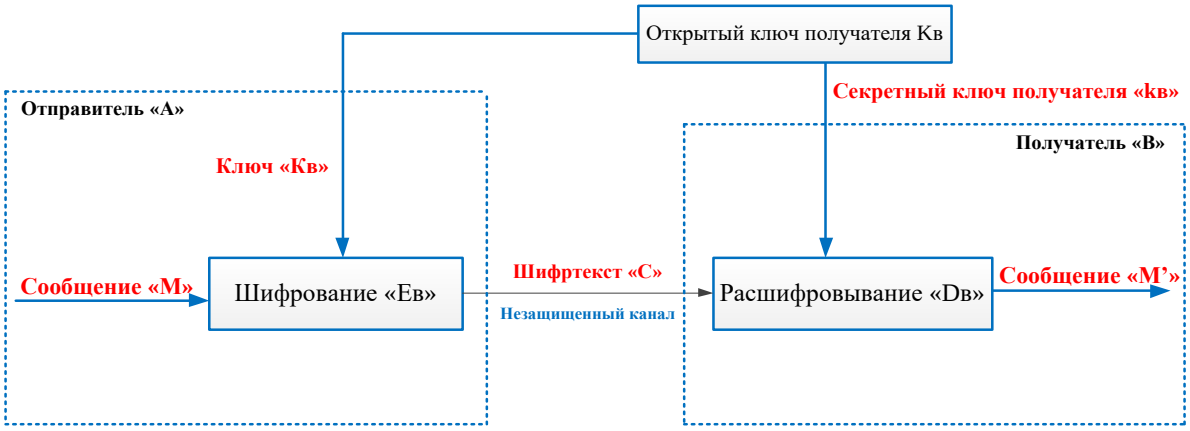

Рисунок 3.3 – Схема асимметричной криптосистемы шифрования

Для криптографического зашифровывания и последующего расшифровывания передаваемой информации используются открытый и секретный ключи получателя «В» сообщения. В качестве ключа зашифровывания должен использоваться открытый ключ получателя, а в качестве ключа расшифровывания – его секретный ключ.

Секретный и открытый ключи генерируются попарно. Секретный ключ должен оставаться у его владельца и быть надежно защищен от НСД. Копия открытого ключа должна находиться у каждого абонента криптографической сети, с которым обменивается информацией владелец секретного ключа. Процесс передачи зашифрованной информации в асимметричной криптосистеме осуществляется следующим образом.

Подготовительный этап.

– абонент «В» генерирует пару ключей: секретный ключ k_B и открытый ключ K_B;

– открытый ключ K_B посылается абоненту «А» и остальным абонентам (или делается доступным, например, на разделяемом ресурсе).

Этап использования.

Использование – обмен информацией между абонентами «А» и «В»:

– абонент «А» зашифровывает сообщение с помощью открытого ключа K_B абонента «В» и отправляет шифртекст абоненту «В»;

– абонент «В» расшифровывает сообщение с помощью своего секретного ключа k_B. Никто другой не может расшифровать данное сообщение, так как не имеет секретного ключа абонента «В». Защита информации в асимметричной криптосистеме основана на секретности ключа k_B получателя сообщения.

Характерные особенности асимметричных криптосистем:

– открытый ключ K_B и криптограмма (шифртекст) «С» могут быть отправлены по незащищенным каналам, т.е. противнику известны K_B и «С»;

– алгоритмы шифрования и расшифровывания, являются открытыми (3.3):

$$\begin{aligned} E_B &: M \to C \\ D_B &: C \to M \end{aligned} \qquad (3.3)$$

Ученые У. Диффи и М. Хеллман сформулировали требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы [32]:

- вычисление пары ключей (K_B, k_B) получателем «В» должно быть простым;
- отправитель «А», зная открытый ключ K_B и сообщение M, может легко вычислить криптограмму C (3.4):

$$C = E_{K_B}(M) \tag{3.4}$$

- получатель «В», используя секретный ключ k_B и криптограмму C, может легко восстановить исходное сообщение M (3.5):

$$M = D_{k_B}(C) \tag{3.5}$$

- противник, зная открытый ключ K_B, при попытке вычислить секретный ключ k_B наталкивается на непреодолимую вычислительную проблему;
- противник, зная пару (K_B, C), при попытке вычислить исходное сообщение M наталкивается на непреодолимую вычислительную проблему.

Концепция асимметричных криптографических систем с открытым ключом основана на применении однонаправленных функций. Однонаправленной функцией называется функция $F(X)$ обладающая двумя свойствами:

– существует алгоритм вычисления значений функции $Y = F(X)$;

– не существует эффективного алгоритма обращения (инвертирования) функции $F(X)$ т.е. (не существует решения уравнения $F(X) = Y$ относительно X.

Как и в случае асимметричных криптографических систем обеспечивается не только конфиденциальность, но также подлинность и целостность передаваемой информации. Подлинность и целостность любого

сообщения обеспечивается формированием цифровой подписи этого сообщения и отправкой в зашифрованном виде сообщения вместе с цифровой подписью. Преимущества асимметричных криптографических систем перед симметричными криптосистемами:

– в асимметричных криптосистемах решена сложная проблема распределения ключей между пользователями, так как каждый пользователь может сгенерировать свою пару ключей сам, а открытые ключи пользователей могут свободно публиковаться и распространяться по сетевым технологиям;

– в асимметричной криптосистеме число используемых ключей связано с числом абонентов линейной зависимостью (в системе из N пользователей используются $2N$ ключей), а не квадратичной, как в симметричных системах;

– асимметричные криптосистемы позволяют реализовать протоколы взаимодействия сторон, которые не доверяют друг другу, поскольку при использовании асимметричных криптосистем закрытый ключ должен быть известен только его владельцу.

Комбинированная криптосистема шифрования. Анализ рассмотренных выше особенностей симметричных и асимметричных криптографических систем показывает, что при совместном использовании они эффективно дополняют друг друга, компенсируя недостатки.

Действительно, главным достоинством асимметричных криптосистем с открытым ключом является их потенциально высокая безопасность, нет необходимости ни передавать, ни сообщать кому-либо значения секретных ключей, ни убеждаться в их подлинности. Однако их быстродействие обычно в сотни (и более) раз меньше быстродействия симметричных криптосистем с секретным ключом. В свою очередь, быстродействующие симметричные криптосистемы страдают существенным недостатком – обновляемый секретный ключ симметричной криптосистемы должен регулярно передаваться партнерам по информационному обмену и во время этих передач возникает опасность раскрытия секретного ключа.

Совместное использование этих криптосистем позволяет эффективно реализовать такую базовую функцию защиты, как криптографическое закрытие передаваемой информации с целью обеспечения ее конфиденциальности. Комбинированное применение симметричного и асимметричного шифрования устраняет основные недостатки, присущие обоим методам, и позволяет сочетать преимущества высокой секретности, предоставляемые асимметричными криптосистемами с открытым ключом, с преимуществами высокой скорости работы, присущими симметричным криптосистемам с секретным ключом. Метод комбинированного использования симметричного и асимметричного шифрования заключается в следующем.

Симметричную криптосистему применяют для шифрования исходного открытого текста, а асимметричную криптосистему с открытым ключом применяют только для шифрования секретного ключа симметричной криптосистемы. В результате асимметричная криптосистема с открытым ключом не заменяет, а лишь дополняет симметричную криптосистему с секретным ключом, позволяя повысить в целом защищенность передаваемой информации. Такой подход иногда называют схемой электронного «цифрового конверта».

Пусть пользователь «А» хочет использовать комбинированный метод шифрования для защищенной передачи сообщения M пользователю «В». Тогда последовательность действий пользователей «А» и «В» будет следующей.

Действия пользователя «А»:

- он создает (например, генерирует случайным образом) сеансовый секретный ключ K_S, который будет использован в алгоритме симметричного шифрования для зашифрования конкретного сообщения или цепочки сообщений;
- зашифровывает симметричным алгоритмом сообщение M на сеансовом секретном ключе K_S;

- зашифровывает асимметричным алгоритмом секретный сеансовый ключ K_S на открытом ключе K_B пользователя «В» (получателя сообщения);
- передает по открытому каналу связи в адрес пользователя «В» зашифрованное сообщение M вместе с зашифрованным сеансовым ключом K_S.

Действия пользователя «А» иллюстрируются схемой шифрования сообщения комбинированным методом (рис.3.4).

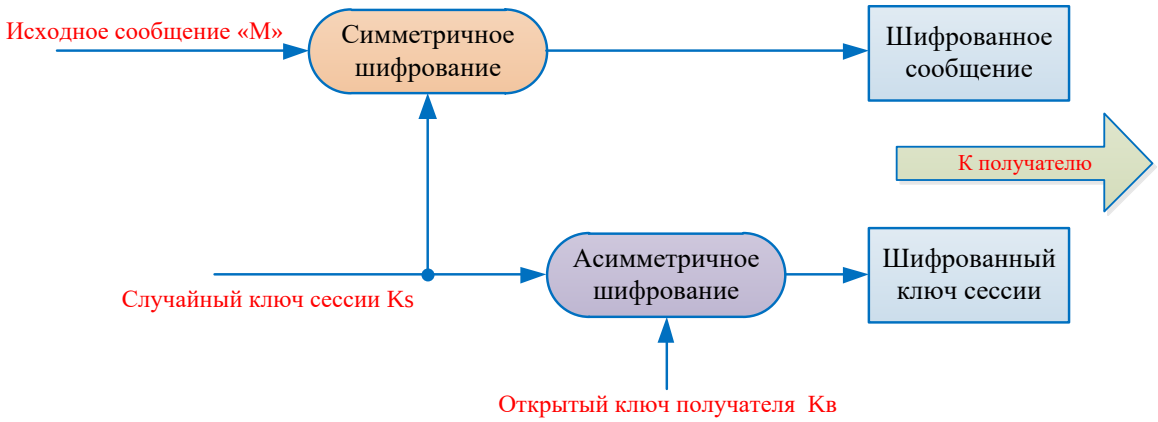

Рисунок 3.4 – Схема шифрования сообщения комбинированным методом (сторона пользователя «А»)

Действия пользователя «В»:

- расшифровывает асимметричным алгоритмом сеансовый ключ K_S с помощью своего секретного ключа k_B;
- расшифровывает симметричным алгоритмом принятое сообщение M с помощью полученного сеансового ключа K_S.

Полученный электронный «цифровой конверт» может раскрыть только законный получатель «В». Только пользователь «В», владеющий личным секретным ключом k_B сможет правильно расшифровать секретный сеансовый ключ K_S и затем с помощью этого ключа расшифровать и прочитать полученное сообщение M. Действия пользователя «В» иллюстрируются схемой расшифровывания сообщения комбинированным методом (рис.3.5).

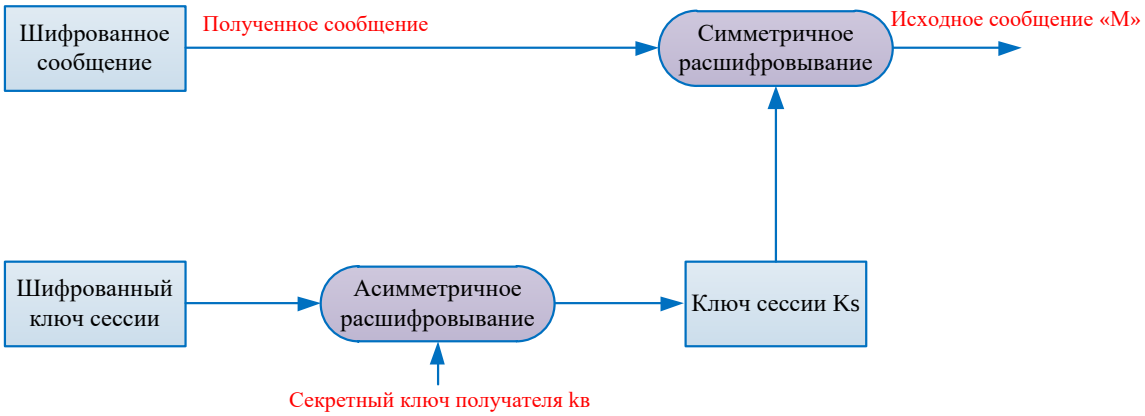

Рисунок 3.5 – Схема шифрования сообщения комбинированным методом (сторона пользователя «B»)

При методе «цифрового конверта» недостатки симметричного и асимметричного криптоалгоритмов компенсируются следующим образом:

- проблема распространения ключей симметричного криптоалгоритма устраняется тем, что сеансовый ключ K_S, на котором шифруются собственно сообщения, передается по открытым каналам связи и зашифрованном виде, для зашифровывания ключа K_S используется асимметричный криптоалгоритм;
- проблема медленной скорости асимметричного шифрования в данном случае практически не возникает, поскольку асимметричным криптоалгоритмом шифруется только короткий ключ K_S, а все данные шифруются быстрым симметричным криптоалгоритмом. В результате получают быстрое шифрование в сочетании с удобным распределением ключей.

Когда требуется реализовать протоколы взаимодействия недоверяющих друг другу сторон, используется следующий способ взаимодействия. Для каждого сообщения на основе случайных параметров генерируется отдельный секретный ключ симметричного шифрования, который и зашифровывается асимметричной системой для передачи вместе с сообщением, зашифрованным этим ключом. В этом случае разглашение ключа симметричного шифрования не будет иметь смысла, так как для

зашифровывания следующего сообщения будет использован другой случайный секретный ключ. При комбинированном методе шифрования применяются криптографические ключи как симметричных, так и асимметричных криптосистем. Очевидно, выбор длин ключей для криптосистемы каждого типа следует осуществлять таким образом, чтобы злоумышленнику было одинаково трудно атаковать любой механизм защиты комбинированной криптосистемы.

Электронная цифровая подпись и функция хэширования. Электронная цифровая подпись используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. При таком обмене существенно снижаются затраты на обработку и хранение документов, убыстряется их поиск. Но возникает проблема аутентификации автора электронного документа и самого документа, т.е. установления подлинности автора и утствия изменений в полученном электронном документе.

Целью аутентификации электронных документов является их защита от возможных видов злоумышленных действий, к которым относятся:

- **активный перехват** – нарушитель, подключившийся к сети, перехватывает документы (файлы) и изменяет их;
- **маскарад** – абонент «С» посылает документ абоненту «В» от имени абонента «А»;
- **ренегатство** – абонент «А» заявляет, что не посылал сообщения абоненту «В», хотя на самом деле послал;
- **подмена –** абонент «В» изменяет или формирует новый документ и заявляет, что получил его от абонента «А»;
- **повтор** – абонент «С» повторяет ранее переданный документ, который абонент «А» посылал абоненту «В»;

Эти виды злоумышленных действий могут нанеси существенный ущерб банковским и коммерческим структурам, государственным предприятиям и организациям, частным лицам, применяющим в своей деятельности ИТ.

Основные процедуры цифровой подписи. Функционально цифровая подпись аналогична обычной рукописной подписи и обладает ее основными достоинствами:

– удостоверяет, что подписанный текст исходит от лица, поставившего подпись;

– не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом.

Электронная цифровая подпись (ЭЦП) – представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом. ЭЦП основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщения, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов сделает невозможным подтверждение подлинности цифровой подписи. ЭЦП реализуется при помощи асимметричных алгоритмов шифрования и хэш-функции.

Технология применения системы ЭЦП предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа. Система ЭЦП включает две основные процедуры:

- формирование цифровой подписи;
- проверки цифровой подписи.

В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи – открытый ключ отправителя.

Процедура формирования цифровой подписи. На подготовительном этапе этой процедуры абонент «А» – отправитель сообщения – генерирует пару ключей: секретный ключ k_A и открытый ключ K_A. Открытый ключ K_A

вычисляется из парного ему секретного ключа k_A. Открытый ключ K_A рассылается остальным абонентам сети (или делается доступным, например, на разделяемом ресурсе) для использования при проверке подписи. Для формирования цифровой подписи отправитель «А» прежде всего, вычисляет значение хэш-функции $h(M)$ подписываемого текста M (рис.3.6).

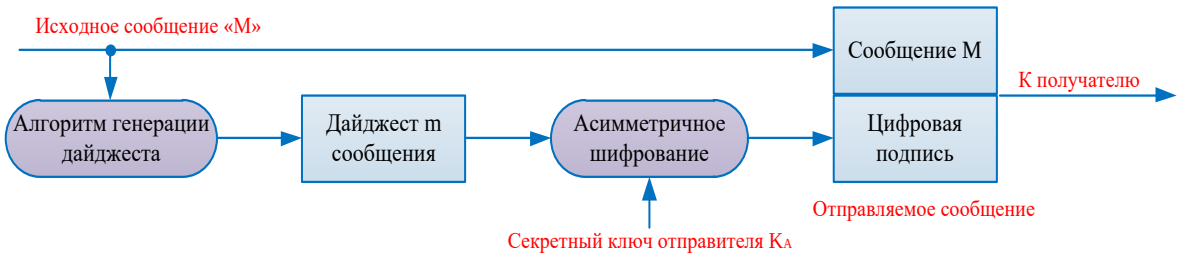

Рисунок 3.6 – Схема формирования электронной цифровой подписи

Хэш-функция служит для сжатия исходного подписываемого текста M в дайджест m – относительно короткое число, состоящее из фиксированного небольшого числа битов и характеризующее весь текст M в целом. Далее отправитель «А» шифрует дайджест m своим секретным ключом k_A. Получаемая при этом пара чисел представляет собой цифровую подпись для данного текста M. Сообщение M вместе с цифровой подписью отправляется в адрес получателя.

Процедура проверки цифровой подписи. Абоненты сети могут проверить цифровую подпись полученного сообщения M с помощью открытого ключа K_A отправителя этого сообщения. При проверке ЭЦП абонент «В» получатель сообщения M – расшифровывает принятый дайджест m открытым ключом K_A отправителя «А». Кроме того, получатель сам вычисляет с помощью хэш-функции $h(M)$ дайджест m' принятого сообщения M и сравнивает его с расшифрованным сообщением. Если m и m' совпадают, то цифровая подпись является подлинной. В противном случае либо подпись подделана, либо изменено содержание сообщения. Принципиальным моментом в системе ЭЦП является невозможность

подделки ЭЦП пользователя без знания его секретного ключа прописывания (рис.3.7).

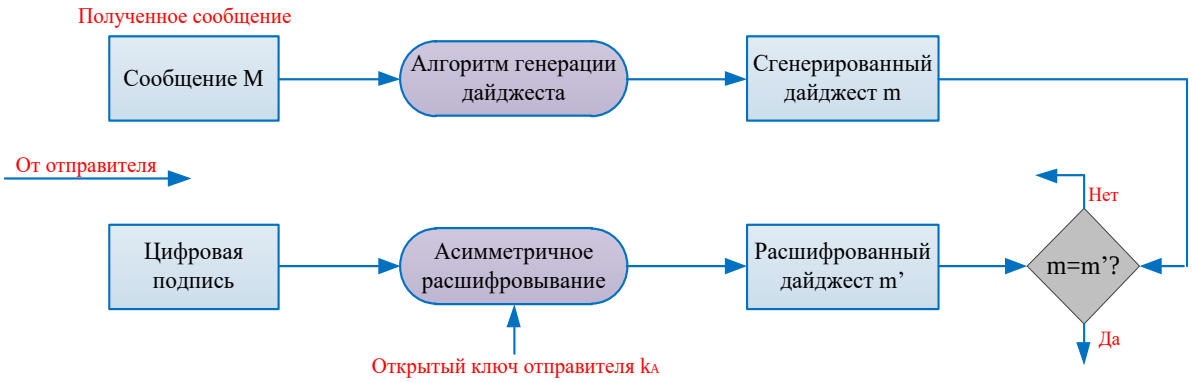

Рисунок 3.7 – Схема формирования электронной цифровой подписи

Поэтому необходимо защитить секретный ключ подписывания от НСД. Секретный ключ ЭЦП аналогично ключу симметричного шифрования рекомендуется хранить на персональном ключевом носителе в защищенном виде. Электронная цифровая подпись представляет собой уникальное число, зависящее от подписываемого документа и секретного ключа абонента. В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путем добавления в него одной или более электронных подписей. Помещаемая в подписываемый файл (или в отдельный файл электронной подписи) структура ЭЦП обычно содержит дополнительную информацию, однозначно идентифицирующую автора подписанного документа. Эта информация добавляется к документу до вычисления ЭЦП, что обеспечивает и ее целостность. Каждая подпись содержит следующую информацию:

– дату подписи;

– срок окончания действия ключа данной подписи;

– информацию о лице, подписавшем файл (Ф.И.О., должность, краткое наименование фирмы);

– идентификатор подписавшего (имя открытого ключа);

– собственно цифровую подпись.

Важно отметить, с точки зрения конечного пользователя процесс формирования и проверки цифровой подписи отличается от процесса криптографического закрытия передаваемых данных следующими особенностями:

– при формировании цифровой подписи используются закрытый ключ отправителя, тогда как при зашифровывании используется открытый ключ получателя. При проверке цифровой подписи используется открытый ключ отправителя, а при расшифровывании – закрытый ключ получателя;

– проверить сформированную подпись может любое лицо, так как ключ проверки подписи является открытым. При положительном результате проверки подписи делается заключение о подлинности и целостности полученного сообщения, т.е. о том, что это сообщение действительно отправлено тем или иным отправителем и не было модифицировано при передаче по сети. Однако, если пользователя интересует, не является ли полученное сообщение повторением ранее отправленного или не было ли оно задержано на пути следования, то он должен проверить дату и время его отправки, а при наличии – порядковый номер.

Аналогично асимметричному шифрованию, необходимо обеспечить невозможность подмены открытого ключа, используемого для проверки ЭЦП. Открытые ключи ЭЦП можно защитить от подмены с помощью соответствующих цифровых сертификатов.

Функция хэширования. Как видно из схемы на рис.3.7, в качестве исходного значения для вычисления ЭЦП берется не сам электронный документ, а его хэш-значение, или дайджест.

Хэш-значение $h(M)$ – это дайджест сообщения M, т.е. сжатое двоичное представление основного сообщения M произвольной длины. Хэш-значение формируется функцией хэширования. Функция хэширования (хэш-функция) представляет собой преобразование, на вход которого подается сообщение переменной длиной M, а выходом является строка фиксированной длины $h(M)$. Иначе говоря, хэш-функция $h(M)$ принимает в

качестве аргумента – сообщение (документ) M произвольной длины и возвращает хэш-значение $H = h(M)$ фиксированной длины (рис.3.8).

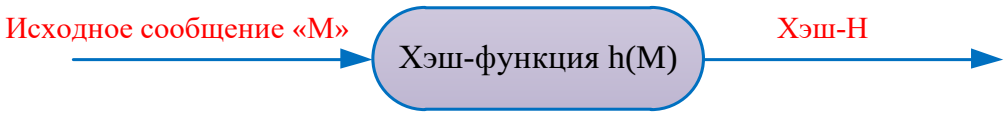

Рисунок 3.8 – Схема формирования хэша $H = h(M)$

Функция хэширования позволяет сжать подписываемый документ M до 128 и более бит (в частности до 128 или 256 бит), тогда как M может быть размером в мегабайт или более. Следует отметить, что значение хэш-функции $h(M)$ зависит сложным образом от документа M и не позволяет восстановить сам документ M. Функция хэширования должна обладать следующими свойствами:

– хэш-функция может быть применена к аргументу любого размера;

– выходное значение хэш-функции имеет фиксированный размер;

– хэш-функцию $h(M)$ достаточно просто вычислить для любого M. Скорость вычисления хэш-функции должна быть такой, чтобы скорость выработки и проверки ЭЦП при использовании хэш-функции была значительно больше, чем при использовании самого сообщения;

– хэш-функция должна быть чувствительна к всевозможным изменениям в тексте M, таким как вставки, выбросы, перестановки и т.п.;

– хэш-функция должна быть однонаправленной, т.е. обладать свойством необратимости, иными словами, задача подбора документа M', который обладал бы требуемым значением хэш-функции, должна быть вычислительно неразрешима;

– вероятность того, что значения хэш-функций двух различных документов (вне зависимости от их длин) совпадут, должна быть ничтожно мала, т.е. для любого фиксированного M с вычислительной точки зрения невозможно найти $M \neq M'$, такое, что $h(M) = h(M')$.

Теоретически возможно, что два различных сообщения могут быть сжаты в одну и ту же свертку (так называемая коллизия, или «столкновение»). Поэтому для обеспечения стойкости функции хэширования необходимо избегать столкновений. Полностью столкновений избежать нельзя, поскольку в общем случае количество возможных сообщений превышает количество возможных выходных значений функции хэширования. Однако вероятность столкновения должна быть низкой. Таким образом, функция хэширования может использоваться для обнаружения изменений сообщения, т.е. может служить для формирования криптографической контрольной суммы (также называемой кодом обнаружения изменений или кодом аутентификации сообщения). В этом качестве хэш-функция используется для контроля целостности сообщения при формировании и проверке ЭЦП.

Хэш-функции широко используются также для аутентификации пользователей. В ряде технологий информационной безопасности применяется своеобразный прием шифрования – шифрование с помощью односторонней хэш-функции. Своеобразие этого шифрования заключается в том, что оно по существу является односторонним, т.е. не сопровождается обратной процедурой – расшифровыванием на приемной стороне. Обе стороны (отправитель и получатель) используют одну и ту же процедуру одностороннего шифрования на основе хэш-функции.

Известные алгоритмы хэширования:

– MD (Message Digest) – ряд алгоритмов хэширования, наиболее распространенных в мире. Например, алгоритм MD5 применяется в последних версиях Microsoft Windows для преобразования пароля пользователя в 16-байтное число;

– SHA1 (Secure Hash Algorithm) – это алгоритм вычисления дайджеста сообщений, вырабатывающий 160-битовый хэш-код входных данных, широко распространен в мире, используется во многих сетевых протоколах защиты информации.

3.2. Антивирусные программы и комплексы. Построение системы антивирусной защиты БИС. Существует много определений компьютерного вируса. Исторически первое определение было дано в 1984 г. Фредом Коэном: «**Компьютерный вирус** – это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно измененной копии, причем последняя сохраняет способность к дальнейшему размножению». Ключевыми понятиями в этом определении являются способность вируса к саморазмножению и способность к модификации вычислительного процесса. Указанные свойства компьютерного вируса аналогичны паразитированию биологического вируса в живой природе. С тех пор острота проблемы вирусов многократно возросла – к концу XX в. в мире насчитывалось более 14500 модификаций компьютерных вирусов. В настоящее время под компьютерным вирусом принято понимать программный код, обладающий следующими свойствами:

– способностью к созданию собственных копий, не обязательно совпадающих с оригиналом, но обладающих свойствами оригинала (самовоспроизведение);

– наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.

Классификация компьютерных вирусов. На сегодняшний день известны десятки тысяч различных компьютерных вирусов. Несмотря на такое изобилие, число типов вирусов, отличающихся друг от друга механизмом распространения и принципом действия, достаточно ограничено. Существуют и комбинированные вирусы, которые можно отнести одновременно к нескольким типам. Вирусы можно разделить на классы [33-40]:

– по среде обитания;

– операционной системе (ОС);

– особенностям алгоритма работы;

– деструктивным возможностям.

Основной и наиболее распространенной классификацией компьютерных вирусов является классификация по среде обитания, или по типам объектов компьютерной системы, в которые внедряются вирусы (рис.3.9). По среде обитания компьютерные вирусы можно разделить:

- на файловые;
- загрузочные;
- макровирусы;
- сетевые.

Рисунок 3.9 – Классификация компьютерных вирусов по среде обитания

Файловые вирусы либо внедряются в выполняемые файлы (наиболее распространенный тип вирусов) различными способами, либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы);

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record). Загрузочные вирусы замещают код программы, получающей управление при загрузке системы. В результате при перезагрузке управление передается вирусу. При этом оригинальный boot-

сектор обычно переносится в какой-либо другой сектор диска. Иногда загрузочные вирусы называют бутовыми вирусами;

Макровирусы заражают макропрограммы и файлы документов современных систем обработки информации, в частности файлы-документы и электронные таблицы популярных редакторов Microsoft Word, Excel и др. Для размножения макровирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла в другие. Вирусы этого типа получают управление при открытии зараженного файла и инфицируют файлы, к которым впоследствии идет обращение из соответствующего офисного приложения;

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Иногда сетевые вирусы называют программами типа «червь». Сетевые черви подразделяются на Internet-черви (распространяются по Internet), LAN-черви (распространяются по локальной сети), IRC-черви (Internet Relay Chat – распространяются по чаты). Существуют также смешанные типы, которые совмещают в себе сразу несколько технологий.

Существуют много комбинированных типов компьютерных вирусов, например, известен «сетевой макро-вирус», который заражает редактируемые документы, а также рассылает свои копии по электронной почте. В качестве другого примера вирусов комбинированного типа можно указать «файлово-загрузочные вирусы», заражающие как файлы, так и загрузочные секторы дисков. Такие вирусы имеют усложненный алгоритм работы и применяют своеобразные методы проникновения в систему.

Жизненный цикл вирусов. Как и у любой программы, у компьютерных вирусов можно выделить **две основные стадии жизненного цикла – хранение и исполнение:**

Стадия хранения соответствует периоду, когда вирус просто хранится на диске совместно с объектом, в который он внедрен. На этой стадии вирус является наиболее уязвимым со стороны антивирусного программного

обеспечения (ПО), так как он не активен и не может контролировать работу операционной системы (ОС) с целью самозащиты. Некоторые вирусы на этой стадии используют механизмы защиты своего кода от обнаружения. Наиболее распространенным способом защиты является шифрование большей части тела вируса. Его использование совместно с механизмами мутации кода делает невозможным выделение сигнатур – устойчивых характеристических фрагментов кода вирусов.

Стадия исполнения компьютерных вирусов, как правило, включает пять этапов:

- загрузка вируса в память;
- поиск жертвы;
- заражение жертвы;
- выполнение деструктивных функций;
- передача управления программе-носителю вируса.

Загрузка вируса в память. Загрузка вируса в память осуществляется ОС одновременно с загрузкой исполняемого объекта, в который вирус внедрен. Например, если пользователь запустил на исполнение программный файл, содержащий вирус, то, очевидно, вирусный код будет загружен в память как часть этого файла. В простейшем случае процесс загрузки вируса представляет собой не что иное, как копирование с диска в оперативную память, сопровождаемое иногда настройкой адресов, после чего происходит передача управления коду тела вируса. Эти действия выполняются ОС, а сам вирус находится в пассивном состоянии. В более сложных ситуациях вирус может после получения управления выполнять дополнительные действия, которые необходимы для его функционирования;

Поиск жертвы. По способу поиска жертвы вирусы можно разделить два класса:

– **к первому классу** относятся вирусы, осуществляющие «активный» поиск с использованием функций ОС. Примером являются файловые вирусы, использующие механизм поиска исполняемых файлов в текущем каталоге;

– **второй класс** составляют вирусы, реализующие «пассивный» механизм поиска, т.е. вирусы, расставляющие «ловушки» для программных файлов. Как правило, файловые вирусы устраивают такие ловушки путем перехвата функции Exec ОС, а макровирусы – с помощью перехвата команд типа Save as из меню File.

Заражение жертвы. В простейшем случае заражение представляет собой самокопирование кода вируса в выбранный в качестве жертвы объект. Классификация вирусов на этом этапе связана с анализом особенностей этого копирования и способов модификации заражаемых объектов. По способу инфицирования жертвы вирусы можно разделить на два класса:

– **к первому классу** относятся вирусы, которые не внедряют свой код непосредственно в программный файл, а изменяют имя файла и создают новый, содержащий тело вируса;

– **второй класс** составляют вирусы, внедряющиеся непосредственно в файлы-жертвы. Они характеризуются местом внедрения.

Выполнение деструктивных функций. Вирусы могут выполнять помимо самокопирования деструктивные функции. По деструктивным возможностям вирусы можно разделить на безвредные, неопасные, опасные и очень опасные:

Безвредные вирусы – это вирусы, в которых реализован только механизм самораспространения. Они не наносят вред системе, за исключением расхода свободной памяти на диске в результате своего распространения;

Неопасные вирусы – это вирусы, присутствие которых в системе связано с различными эффектами и уменьшением свободной памяти на диске, но которые не наносят вред программам и данным;

Опасные вирусы – это вирусы, которые могут привести к серьезным сбоям в работе компьютера. Последствием сбоя могут стать разрушение программ и данных;

Очень опасные вирусы – это вирусы, в алгоритм работы которых заведомо заложены процедуры, непосредственно приводящие к разрушениям программ и данных, а также к стиранию информации, записанной в системных областях памяти и необходимой для работы компьютера.

Передача управления программе-носителю вируса. Тут следует указать на деление вирусов на разрушающие и неразрушающие:

Разрушающие вирусы не заботятся о сохранении работоспособности зараженных программ, поэтому для них этот этап функционирования утствует.

Для неразрушающих вирусов этот этап связан с восстановлением в памяти программы в том виде, в котором она должна корректно исполняться, и передачей управления программе-носителю вируса.

Вредоносные программы других типов. Кроме вирусов принято выделять еще несколько видов вредоносных программ. Это троянские программы, логические бомбы, хакерские утилиты скрытого администрирования удаленных компьютеров, программы, ворующие пароли доступа к ресурсам Internet и прочую конфиденциальную информацию. Четкого разделения между ними не существует: троянские программы могут содержать вирусы, в вирусы могут быть встроены логические бомбы и т.д.

Троянские программы не размножаются и не рассылаются сами. Внешне они выглядят совершенно безобидно и даже предлагают полезные функции. Но когда пользователь загрузит такую программу в свой компьютер и запустит ее, она может незаметно выполнять вредоносные функции. Чаще всего троянские программы используются для первоначального распространения вирусов, для получения удаленного доступа к компьютеру через Internet, кражи данных или их уничтожения.

Логической бомбой называется программа или ее отдельные модули, которые при определенных условиях выполняют вредоносные действия. Логическая бомба может, например, сработать по достижении определенной даты или тогда, когда в базе данных (БД) появится или исчезнет запись, и т.п.

Такая бомба может быть встроена в вирусы, троянские программы и даже в обычные программы.

Антивирусные программы и комплексы. Для защиты от компьютерных вирусов могут использоваться:

- общие методы и средства защиты информации;
- специализированные программы для защиты от вирусов;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусами.

Общие методы и средства защиты информации полезны не только для защиты от вирусов. Они используются также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя. Существует две основные разновидности этих средств:

– средства копирования информации (применяются для создания копий файлов и системных областей дисков);

– средства разграничения доступа (предотвращают несанкционированное использование информации, в частности обеспечивают защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей).

При заражении компьютера вирусом важно его обнаружить. К внешним признакам проявления деятельности вирусов можно отнести следующие:

– вывод на экран непредусмотренных сообщений или изображений;

– подача непредусмотренных звуковых сигналов;

– изменение даты и времени модификации файлов;

– исчезновение файлов и каталогов или искажение их содержимого;

– частые зависания и сбои в работе компьютера;

– медленная работа компьютера;

– невозможность загрузки ОС;

– существенное уменьшение размера свободной оперативной памяти;

– прекращение работы или неправильная работа ранее успешно функционировавших программ;

– изменение размеров файлов;

– неожиданное значительное увеличение количества файлов на диске.

Однако следует заметить, что перечисленные выше явления необязательно вызываются действиями вируса, они могут быть следствием и других причин. Поэтому правильная диагностика состояния компьютера всегда затруднена и обычно требует привлечения специализированных программ.

Антивирусные программы. Для обнаружения и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать компьютерные вирусы. Практические все антивирусные программы обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов. **Задачи антивирусной программы:**

– препятствовать проникновению зараженной информации в компьютерную систему;

– минимизировать последствия от вирусов, которые смогли проникнуть в систему персонального компьютера;

– обнаружить источник возникшего вируса;

– удалить и нейтрализовать вредоносные файлы.

Антивирусные программы используют различные методы обнаружения вирусов:

- метод сравнения с эталоном;
- эвристический анализ;
- антивирусный мониторинг;
- метод обнаружения изменений;
- встраивание антивирусов в BIOS компьютера.

Метод сравнения с эталоном. Самый простой метод обнаружения заключается в том, что для поиска известных вирусов используются так называемые маски. Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Антивирусная программа последовательно сканирует проверяемые файлы в поиске масок известных вирусов. Антивирусные сканеры способны найти только уже известные вирусы, для которых определена маска. Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы. Применение простых сканеров не защищает компьютер от проникновения новых вирусов. Для шифрующихся и полиморфных вирусов, способных полностью изменять свой код при заражении новой программы или загрузочного сектора, невозможно выделить маску, поэтому антивирусные сканеры их не обнаруживают.

Эвристический анализ. Для того чтобы размножаться, компьютерный вирус должен совершать какие-то конкретные действия: копирование в память, запись в секторы и т.д. Эвристический анализатор содержит список таких действий и проверяет программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов. Эвристический анализатор может обнаружить, например, что проверяемая программа устанавливает резидентный модуль в памяти или записывает данные в исполнимый файл программы. Обнаружив зараженный файл, анализатор, обычно выводит сообщение на экране монитора и делает запись в собственном или системном журнале. В зависимости от настроек, антивирус может также направлять сообщение об обнаруженном вирусе администратору сети. Эвристический анализ позволяет обнаруживать неизвестные ранее вирусы. Первый эвристический анализатор появился в начале 1990-х гг. Практически все современные антивирусные программы реализуют собственные методы эвристического анализа. В качестве примера такой программы можно указать сканер McAffee Virus Scan.

Антивирусный мониторинг. Суть данного метода состоит в том, что в памяти компьютера постоянно находится антивирусная программа, осуществляющая мониторинг всех подозрительных действий, выполняемых другими программами. Антивирусный мониторинг позволяет проверять все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Internet или скопированные на жесткий диск с дискеты либо компакт диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие. Пример такой программы – Spider Guard, который входит в комплект сканера Doctor Web и выполняет функции антивирусного монитора.

Метод обнаружения изменений. При реализации этого метода антивирусные программы, называемые ревизорами диска, запоминают предварительно характеристики всех областей диска, которые могут подвергнуться атаку, а затем периодически проверяют их. Заражая компьютер, вирус изменяет содержимое жесткого диска, например, дописывает свой код в файл программы или документа, добавляет вызов программы-вируса в файл AUTOEXEC.BAT, изменяет загрузочный сектор, создает файл-спутник. При сопоставлении значений характеристик областей диска антивирусная программа может обнаружить изменения, сделанные как известным, так и неизвестным вирусом.

Встраивание антивирусов в BIOS компьютера. В системные платы компьютеров встраивают простейшие средства защиты от вирусов. Эти средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет. Если какая-либо программа пытается изменить содержимое загрузочных секторов, срабатывает защита, и пользователь получает соответствующее предупреждение. Однако эта защита не очень надежна. Известны вирусы, которые пытаются отключить антивирусный контроль BIOS, изменяя

некоторые ячейки в энергонезависимой памяти (CMOS – complementary metal-oxide semiconductor) компьютера.

Различают следующие виды антивирусных программ:

- программы-фаги (сканеры);
- программы-ревизоры (CRC-сканеры);
- программы-блокировщики;
- программы-иммунизаторы.

Программы-фаги (сканеры) используют для обнаружения вирусов метод сравнения с эталоном, метод эвристического анализа и некоторые другие методы. Программы-фаги осуществляют поиск характерной для конкретного вируса маски путем сканирования в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Программы-фаги не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале работы программы-фаги сканируют оперативную память, обнаруживают вирусы и уничтожают их и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги – программы-фаги, предназначенные для поиска и уничтожения большого числа вирусов.

Программы-фаги делятся также на резидентные мониторы, производящие сканирование, и нерезидентные сканеры, обеспечивающие проверку системы только по запросу. Резидентные мониторы обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как нерезидентный сканер способен опознать вирус только во время своего очередного запуска. К достоинствам программ-фагов всех типов относится их универсальность. К недостаткам следует отнести относительно небольшую скорость поиска вирусов и относительно большие размеры антивирусных баз. Наиболее известные программы-фаги: Aidstest, Scan, Norton Antivirus, Doctor Web. Учитывая, что постоянно

появляются новые вирусы, программы-фаги быстро устаревают, и требуется регулярное обновление версий.

Программы-ревизоры (CRC-сканеры) используют для поиска вирусов метод обнаружения изменений. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (Cyclic redundancy check – циклический избыточный код) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы, а также некоторая другая информация (длины файлов, даты их последней модификации и др.) затем сохраняются в БД антивируса. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в БД, с реально подсчитанными значениями. Если информация о файле, записанная в БД, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом. Как правило, сравнение состояний производят сразу после загрузки ОС. CRC-сканеры, использующие алгоритмы анти-стелс, являются довольно мощным средством против вирусов практически: 100% вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у CRC-сканеров имеется недостаток, заметно снижающий их эффективность: они не могут определить вирус в новых файлах (в электронной почте, на дисках, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их БД утствует информация об этих файлах. К числу CRC-сканеров относится широко распространенная в странах СНГ (Содружество независимых государств) программа ADinf (Advanced Diskinfoscope) и ревизор AVP Inspector. Вместе с ADinf применяется лечащий модуль ADinf Cure Module (ADinfExt), который использует собранную ранее информацию о файлах для их восстановления после поражения неизвестными вирусами. В состав ревизора AVP Inspector также входит лечащий модуль, способный удалять вирусы.

Программы-блокировщики реализуют метод антивирусного мониторинга. Антивирусные блокировщики – это резидентные программы, перехватывающие «вирусо-опасные» ситуации и сообщающие об этом

пользователю. К «вирусо-опасным» ситуациям относятся вызовы, которые характерны для вирусов в моменты их размножения (вызовы на открытие для записи в выполняемые файлы, запись в загрузочные секторы дисков или MBR (Master Boot Record) винчестера, попытки программ остаться резидентно и т.п.). При попытке какой-либо программы произвести указанные действия блокировщик посылает пользователю сообщение и предлагает запретить соответствующее действие. К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения, что бывает особенно полезно в случаях, когда регулярно появляется давно известный вирус. Однако они не «лечат» файлы и диски. Для уничтожения вирусов требуется применять другие программы, например фаги. К недостаткам блокировщиков можно отнести существование путей обхода их защиты и их «назойливость» (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла). Следует отметить, что созданы антивирусные блокировщики, выполненные в виде аппаратных компонентов компьютера. Наиболее распространенной является встроенная в BIOS защита от записи в MBR винчестера.

Программы-иммунизаторы это программы, предотвращающие заражение файлов. Иммунизаторы делятся на два типа: иммунизаторы – сообщающие о заражении, и иммунизаторы – блокирующие заражение каким-либо типом вируса. Иммунизатор первого типа обычно записываются в конец файлов и при запуске файла каждый раз проверяют его на изменение. Иммунизатор второго типа защищает систему от поражения вирусом определенного вида. Он модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, вирус при этом воспринимает их зараженными и поэтому не внедряется. Такой тип иммунизации не может быть универсальным, поскольку нельзя иммунизировать файлы от всех известных вирусов. Однако в качестве полумеры подобные иммунизаторы могут вполне надежно защитить компьютер от нового неизвестного вируса

вплоть до того момента, когда он будет определяться антивирусными сканерами.

Профилактические меры защиты. Своевременное обнаружение зараженных вирусами файлом и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения «вирусной эпидемии» на другие компьютеры. Абсолютно надежных программ, гарантирующих обнаружение и уничтожение любого вируса, не существует. Важным методом борьбы с компьютерными вирусами является своевременная профилактика. Чтобы существенно уменьшить вероятность заражения вирусом и обеспечить надежное хранение информации на дисках, необходимо выполнять следующие меры профилактики:

– применять только лицензионные программные обеспечения (ПО);

– оснастить компьютер современными антивирусными программами и постоянно возобновлять их версии;

– всегда проверять диски на наличие вирусов;

– при переносе на свой компьютер файлов в архивированном виде проверять их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;

– периодически проверять на наличие вирусов жесткие диски компьютера;

– всегда защищать свои диски (флешки) от записи при работе на других компьютерах, если на них не будет производиться запись информации;

– обязательно делать на флешках архивные копии ценной для пользователя информации;

– использовать антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей.

Антивирусные программные комплексы. У каждого типа антивирусных программ есть свои достоинства и недостатки. Только комплексное использование нескольких типов антивирусных программ

может привести к приемлемому результату. Программные средства защиты представляют собой комплекс алгоритмов и программ, нацеленных на контроль и исключение проникновения несанкционированной информации. Существует спектр программных комплексов, предназначенных для профилактики заражения вирусом, обнаружения и уничтожения вирусов. Они обладают универсальностью, гибкостью, адаптивностью и др.

Перечислим наиболее распространенные антивирусные программные комплексы:

– Bitdefender;

– Kaspersky;

– Norton;

– McAfee;

– Avast;

– Avira;

– Windows Defender;

– Trend Micro;

– TotalAV;

– Dr.Web.

Центральный Банк Республики Узбекистан в настоящее время активно сотрудничает с компанией «Лаборатория Касперского» в области защиты банковских информационных систем от киберугроз [3]. «Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности и цифровой приватности с 1997 года. Обширное портфолио «Лаборатория Касперского» включает в себя передовые технологии для защиты конечных устройств, ряд специализированных продуктов и сервисов, а также кибериммунные решения для борьбы со сложными и постоянно эволюционирующими киберугрозами. Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 220 тысяч корпоративных клиентов во всем мире [5]. Решения «Лаборатории Касперского» имеют сертификаты

соответствия ФСТЭК России и ФСБ (Федеральная служба безопасности), включены в единый реестр Российского ПО, а также полностью соответствуют требованиям закона о защите персональных данных, предъявляемым к антивирусным продуктам. Все это дает возможность их использования в организациях с повышенными требованиями к уровню безопасности и защите данных, в том числе составляющих государственную тайну.

Построение системы антивирусной защиты БИС. Проблема антивирусной защиты – одна из приоритетных проблем обеспечения безопасности корпоративных информационных ресурсов организации, банковская информационная система (БИС) по сути, также является корпоративной компьютерной сетью. Ее актуальность объясняется:

– лавинообразным ростом числа компьютерных вирусов;

– неудовлетворительным состоянием антивирусной защиты в существующих корпоративных компьютерных сетях. Сегодня сети Центрального Банка находятся в постоянном развитии. Однако вместе с ним постоянно растет и число точек проникновения вирусов в корпоративные сети Intranet. Как правило, такими точками являются: шлюзы и серверы Internet, серверы файлов/приложений, серверы корпоративной электронной почты, рабочие станции.

Для небольших предприятий (банков), использующих до 10 узлов, целесообразны решения по антивирусной защите, имеющие удобный графический интерфейс и допускающие локальное конфигурирование без применения централизованного управления. Для крупных предприятий (банков) предпочтительнее системы антивирусной защиты с несколькими консолями и менеджерами управления, подчиненными некоторому единому общему центру. Такие решения позволяют обеспечить оперативное централизованное управление локальными антивирусными клиентами и дают возможность при необходимости интегрироваться с другими решениями в области безопасности корпоративных сетей.

3.3. Аппаратно-технические способы защиты информации в БИС.

В работах [6-13, 27-49] приведены основные виды кибератак и способы защиты от них. Анализ результатов, описанных в этих работах, показывает, что наиболее целесообразными для использования в банковских информационных системах являются меры, направленные на защиту сетевых элементов от угроз, связанных с реализацией злоумышленником DDoS и других видов кибератак, а именно:

Предотвращение атаки – необходимо проводить профилактику и анализ причин, которые приводят к проведению теми или иным лицами DDoS-атак. Личная неприязнь, конкуренция, религиозные или политические разногласия, а также многие другие факторы могут стать причиной такой атаки. Если вовремя устранить причины таких атак и сделать соответствующие выводы, то в дальнейшем удастся избежать повторения ситуации. Данный метод нацелен на защиту практически от любых DDoS-атак, так как является управленческим, а не техническим решением;

Ответные меры – необходимо применять активные меры воздействия на источники или на организаторов атак, используя как технические, так и организационно-правовые методы. Некоторые фирмы представляют сервис поиска организатора атак, который позволяет вычислить не только человека, проводящего атаку, но и заказчика данной атаки;

Специализированное программно-аппаратное обеспечение. Хотя атака возможна на любом из уровней ISO/OSI (ЭМВОС), особой популярностью пользуются атаки на 3-4 и 7 уровнях ЭМВОС модели. DDoS-атаки на 3-м и 4-м уровне – (инфраструктурные), основаны на использовании большого объема, мощного потока данных (flood) на транспортном уровне, чтобы замедлить работу веб-сервера, грузить канал и в итоге, ограничить доступ других пользователей к ресурсу. Эти типы атак, как правило, включают ICMP, SYN и UDP flood. DDoS-атака 7-го уровня заключается в перегрузке отдельных элементов инфраструктуры сервера приложений. Атаки 7-го уровня особенно сложны, скрыты и трудны для выявления, так

как имеют сходство с полезным веб-трафиком. Даже самые простые атаки 7-го уровня, к примеру, попытки войти в систему под произвольным именем пользователя и паролем или повторяющийся произвольный поиск на динамических веб-страницах, могут критически загрузить CPU и базы данных. Также, используя DDoS-атаки, злоумышленники могут многократно изменять сигнатуры атак 7-го уровня, еще их еще более усложняя их распознавание и пересечение.

Для защиты от DDoS-атаки на 4–7 уровнях используются – сетевые экраны, ограничения сеанса, SYN-cookie, а на 3–4 уровнях – линейные списки контроля доступа, ограничение скорости. Сейчас многие производители программного и аппаратного обеспечения предлагают готовые решения для защиты от DDoS-атак. Такое программное и аппаратное обеспечение может выглядеть как небольшой сервер, который позволяет защититься от слабых и средних DDoS-атак. **На практике часто используется следующее оборудование для устранения DDoS-атак:**

– брандмауэры с динамической проверкой пакетов;

– динамические механизмы SYN-прокси;

– ограничение количества SYN за секунду для каждого IP-адреса;

– ограничение количество SYN за секунду для каждого удаленного IP-адреса;

– установка экранов ICMP flood на брандмауэре;

– установка экранов UDP flood на брандмауэре;

– ограничение скорости роутеров, примыкающих к брандмауэрам и сети.

Фильтрация и блокировка трафика, исходящего от атакующих машин, позволяет снизить или вовсе нейтрализовать атаку. При использовании этого метода входящий трафик фильтруется в соответствии с теми или иными правилами, заданными при установке фильтров. Можно выделить два способа фильтрации: маршрутизацию по списками ACL и использование межсетевых экранов.

Использование списков ACL позволяет фильтровать второстепенные протоколы, не затрагивая при этом протоколы TCP и не замедляя скорости работы пользователей с ресурсом. Однако при использовании злоумышленниками первостепенных запросов или ботнет, данный способ фильтрации окажется неэффективным. **Межсетевые экраны являются крайне эффективным способом защиты от DDoS и других видов кибератак.**

Межсетевой экран (МЭ) – это специализированный комплекс межсетевой защиты, называемый также брандмауэром или системой firewall. МЭ позволяет разделить общую сеть на две части (или более) и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной сетью (БИС) и глобальной сетью Internet. Обычно МЭ защищают внутреннюю сеть предприятия от «вторжений» из глобальной сети Internet, хотя они могут использоваться и для защиты от кибератаки из корпоративной Intranet. Технология МЭ одна из самых первых технологий защиты корпоративных сетей от внешних угроз. Для большинства организаций установка МЭ является необходимым условием обеспечения безопасности внутренней сети.

Функции межсетевого экрана. Для противодействия несанкционированному межсетевому доступу МЭ должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (см. рис.3.10). При этом все взаимодействия между этими сетями должны осуществляться только через МЭ. Организационно МЭ входит в состав защищаемой сети. МЭ защищающий сразу множество узлов внутренней сети, призван решить:

– задачу ограничения доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи,

сотрудники банков, хакеры пытающиеся получить доступ к серверам баз данных, защищаемых МЭ;

– задачу разграничения доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регулировать доступ к серверам, не требующимся для выполнения служебных обязанностей (рис.3.10).

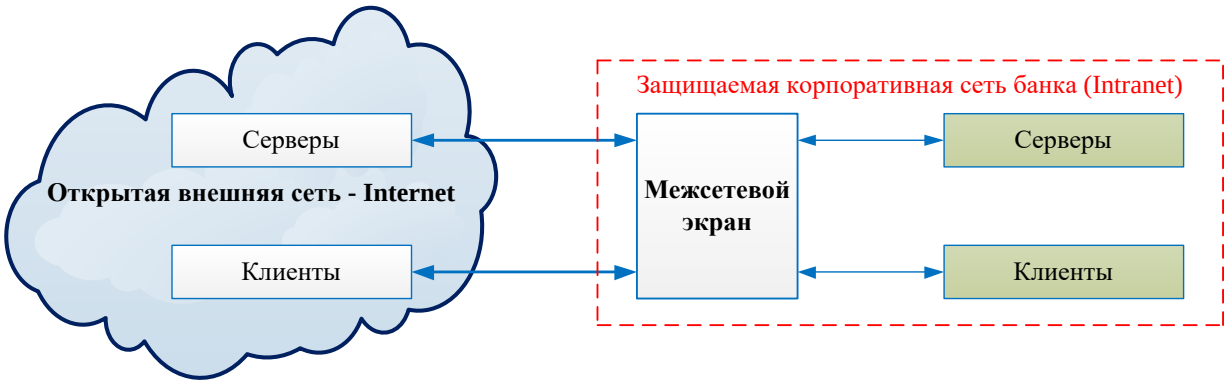

Рисунок 3.10 – Схема подключения межсетевого экрана

До сих пор не существует единой общепризнанной классификации МЭ. Их можно классифицировать, например, по следующим основным признакам [40].

По функционированию на уровнях модели OSI:

– пакетный фильтр (screen int router);

– шлюз сеансового уровня;

– прикладной шлюз (application gateway);

– шлюз экспертного уровня (stateful inspection firewall).

По используемой технологии:

– контроль состояния протокола (stateful inspection);

– на основе модулей посредников (proxy).

По исполнению:

– аппаратно-программный;

– программный.

По схеме подключения:

– схема единой защиты сети;

– схема с защищаемым закрытым и не защищаемым открытым сегментами сети;

– схема с раздельной защитой закрытого и открытого сегментов сети.

Пакетный фильтр. Фильтрация информационных потоков состоит в их выборочном пропускании через экран, возможно, с выполнением некоторых преобразований. Фильтрация осуществляется на основе набора предварительно загруженных в МЭ правил, соответствующих принятой политике безопасности. Поэтому МЭ удобно представлять как последовательность фильтров, обрабатывающих информационный поток (рис.3.11).

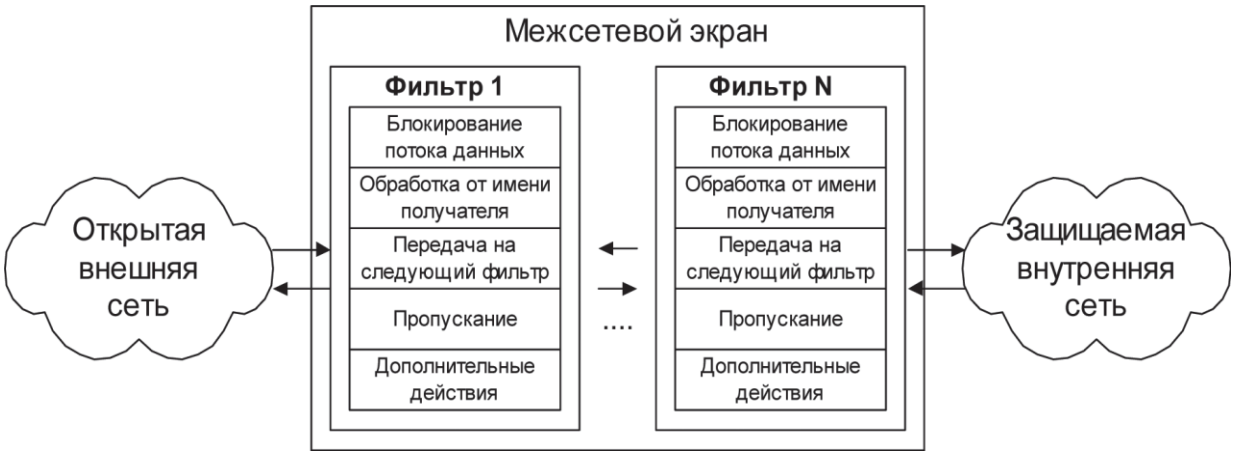

Рисунок 3.11 – Структура межсетевого экрана

Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем:

- анализа информации по заданным в интерпретируемых правилах критериям, например по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена;
- принятия на основе интерпретируемых правил одного из следующих решений:

– не пропустить данные;

– обработать данные от имени получателя и возвратить результат отправителю;

– передать данные на следующий фильтр для продолжения анализа;

– пропустить данные, игнорируя следующие фильтры.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например, мер преобразование данных, регистрация событий и др. Соответственно правила фильтрации определяют перечень условий, по которым осуществляется:

– разрешение или запрещение дальнейшей передачи данных;

– выполнение дополнительных защитных функций.

В качестве критериев анализа информационного потока могут использоваться следующие параметры:

– служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;

– непосредственное содержимое пакетов сообщений, проверяемое например, на наличие компьютерных вирусов;

– внешние характеристики потока информации, например, временные, частотные характеристики, объем данных и т.д.

Используемые критерии анализа зависят от уровней модели OSI, на которых осуществляется фильтрация. В общем случае, чем выше уровень модели OSI, на котором МЭ фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты.

Выполнение функций посредничества. Функции посредничества МЭ выполняет с помощью специальных программ, называемых экранирующими агентами или программами-посредниками. Эти программы являются резидентными и запрещают непосредственную передачу пакетов сообщений между внешней и внутренней сетью. В общем случае программы-посредники, блокируя прозрачную передачу потока сообщений, могут выполнять следующие функции:

– проверку подлинности передаваемых данных;

– фильтрацию и преобразование потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;

– разграничение доступа к ресурсам внутренней сети;

– разграничение доступа к ресурсам внешней сети;

– кэширование данных, запрашиваемых из внешней сети;

– идентификацию и аутентификацию пользователей;

– трансляцию внутренних сетевых адресов для исходящих пакетов сообщений;

– регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов.

Программы-посредники могут осуществлять проверку подлинности получаемых и передаваемых данных. Это актуально не только для аутентификации электронных сообщений, но и мигрирующих программ (Java, ActiveX Controls), по отношению к которым может быть выполнен подлог. Проверка подлинности сообщений и программ заключается в контроле их цифровых подписей.

Способы разграничения доступа к ресурсам внутренней сети практически не отличаются от способов разграничения, поддерживаемых на уровне операционной системы. При разграничении доступа к ресурсам внешней сети чаще всего используется один из следующих подходов:

– разрешение доступа только по заданным адресам во внешней сети;

– фильтрация запросов на основе обновляемых списков недопустимых адресов и блокировка поиска информационных ресурсов по нежелательным ключевым словам;

– накопление и обновление администратором санкционированных информационных ресурсов внешней сети в дисковой памяти МЭ и полный запрет доступа во внешнюю сеть.

С помощью специальных посредников поддерживается также кэширование данных, запрашиваемых из внешней сети. При доступе

пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на пространстве жесткого диска МЭ, называемого в этом случае proxy-сервером. Поэтому если при очередном запросе нужная информация окажется на proxy-сервере, то посредник предоставляет ее без обращения к внешней сети, что существенно ускоряет доступ. Администратору следует позаботиться только о периодическом обновлении содержимого proxy-сервера.

Особенности функционирования МЭ на различных уровнях модели OSI. МЭ поддерживают безопасность межсетевого взаимодействия на различных уровнях модели OSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Поэтому комплексный МЭ удобно представить в виде совокупности неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI. Чаще всего комплексный экран функционирует на сетевом, сеансовом и прикладном уровнях эталонной модели. Соответственно различают такие неделимые МЭ (рис.3.12), как:

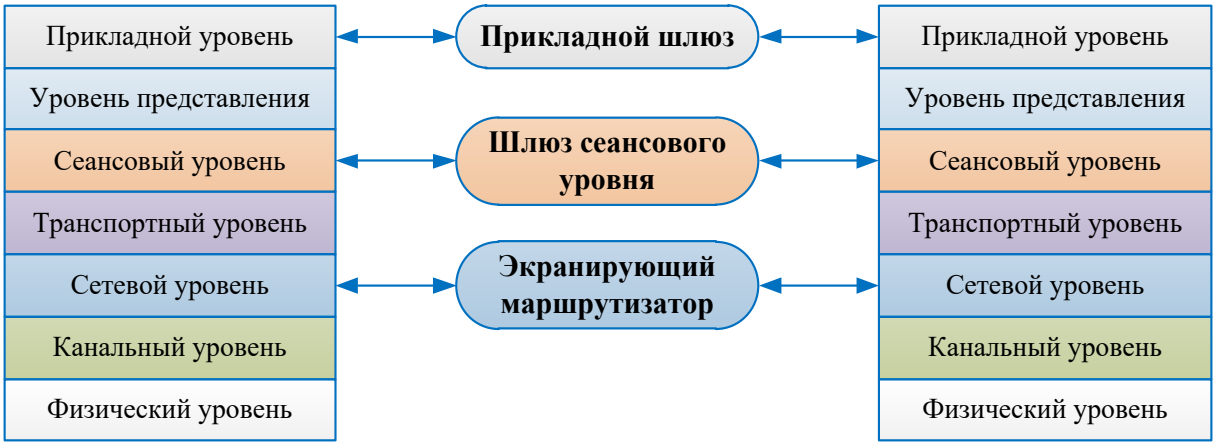

Рисунок 3.12 – Типы межсетевых экранов функционирующих на отдельных уровнях модели OSI

– экранирующий маршрутизатор;

– шлюз сеансового уровня (экранирующий транспорт);

– шлюз прикладного уровня (экранирующий шлюз).

Используемые в сетях протоколы (TCP/IP, SPX/IPX) не полностью соответствуют эталонной модели OSI, поэтому экраны перечисленных типов при выполнении своих функций могут охватывать и соседние уровни эталонной модели. Например, прикладной экран может осуществлять автоматическое зашифровывание сообщений при их передаче во внешнюю сеть, а также автоматическое расшифровывание криптографически закрытых применяемых данных. В этом случае такой экран функционирует не только на прикладном уровне модели OSI, но и на уровне представления.

Шлюз сеансового уровня при своем функционировании охватывает транспортный и сетевой уровни модели OSI. Экранирующий маршрутизатор при анализе пакетов сообщений проверяет их заголовки не только сетевого, но и транспортного уровня. МЭ указанных типов имеют свои достоинства и недостатки. Многие из используемых МЭ являются либо прикладными шлюзами, либо экранирующими маршрутизаторами, не обеспечивая полную безопасность межсетевого взаимодействия. Надежную защиту обеспечивают только комплексные межсетевые экраны, каждый из которых объединяет экранирующий маршрутизатор, шлюз сеансового уровня, а также прикладной шлюз.

Прикладной шлюз. Прикладной шлюз, называемый также экранирующим шлюзом, функционирует на прикладном уровне модели OSI, охватывая также уровень представления, и обеспечивает наиболее надежную защиту межсетевых взаимодействий. Защитные функции прикладного шлюза, как и шлюза сеансового уровня, относятся к функциям посредничества. Однако прикладной шлюз, в отличие от шлюза сеансового уровня, может выполнять существенно большее количество функций защиты, к которым относятся следующие:

– идентификация и аутентификация пользователей при попытке установления соединений через МЭ;

– проверка подлинности информации, передаваемой через шлюз;

– разграничение доступа к ресурсам внутренней и внешней сетей;

– фильтрация и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации;

– регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерация отчетов.

Поскольку функции прикладного шлюза относятся к функциям посредничества, этот шлюз представляет собой универсальный компьютер, на котором функционируют программные посредники – по одному для каждого обслуживаемого прикладного протокола (HTTP, FTP, SMTP, NNTP и др.). Программный посредник (application proxy) каждой службы TCP/IP ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе. Прикладной шлюз перехватывает с помощью соответствующих экранирующих агентов входящие и исходящие пакеты, копирует и перенаправляет информацию, т.е. функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетью (рис.3.13).

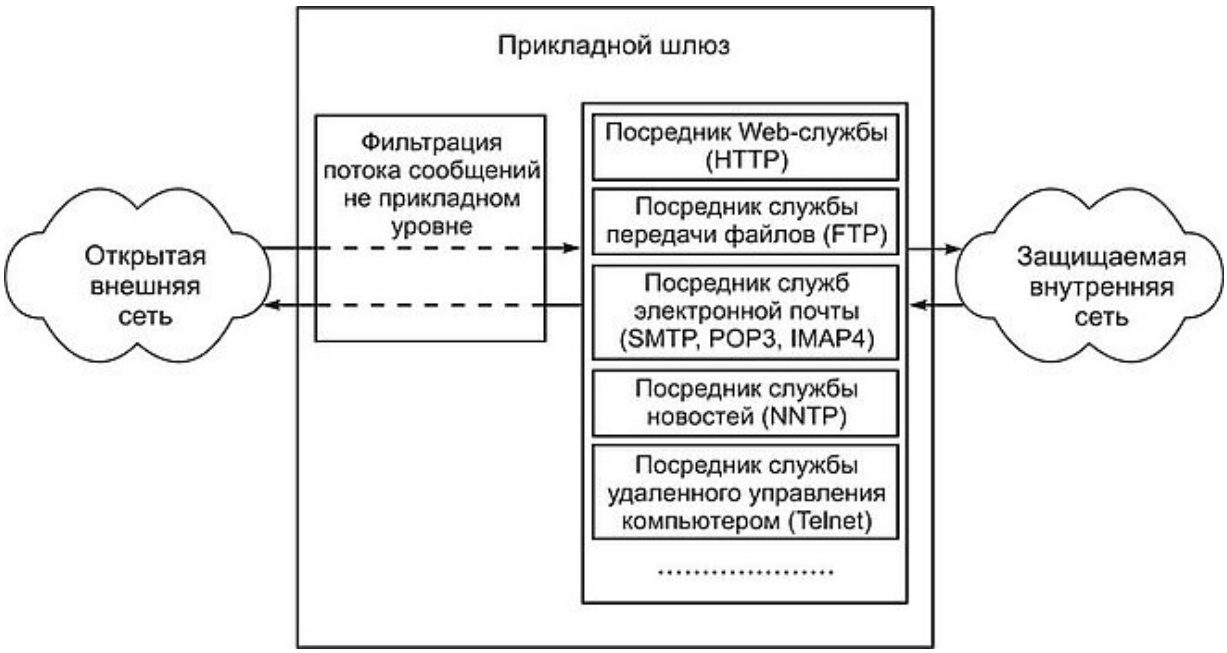

Рисунок 3.13 – Схема функционирования прикладного шлюза

Посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уровня.

Прикладные шлюзы используют в качестве посредников специально разработанные для этой цели программные серверы конкретных служб TCP/IP – серверы HTTP (HTTPS), FTP, SMTP, NNTP и др. Эти программные серверы функционируют на МЭ в резидентном режиме и реализуют функции защиты, относящиеся к соответствующим службам TCP/IP. Шлюз прикладного уровня обладает следующими достоинствами:

– обеспечивает высокий уровень защиты локальной сети благодаря возможности выполнения большинства функций посредничества;

– защита на уровне приложений позволяет осуществлять большое число дополнительных проверок, уменьшая тем самым вероятность проведения успешных атак, возможных из-за недостатков программного обеспечения;

– при нарушении его работоспособности блокируется сквозное прохождение пакетов между разделяемыми сетями, в результате чего безопасность защищаемой сети не снижается из-за возникновения отказов.

Схемы сетевой защиты на базе МЭ. При подключении корпоративной сети (БИС) к глобальным сетям необходимы:

– защита корпоративной или локальной сети от удаленного НСД со стороны глобальной сети;

– разграничение доступа в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную сеть.

Для эффективной защиты межсетевого взаимодействия система МЭ должна быть правильно установлена и сконфигурирована. Данный процесс состоит:

- из формирования политики межсетевого взаимодействия;
- выбора схемы подключения и настройки параметров функционирования МЭ.

Формирование политики межсетевого взаимодействия. Политика межсетевого взаимодействия является составной частью общей политики безопасности в банках (организациях). Она определяет требования к

безопасности информационного обмена организации с внешним миром и должна отражать два аспекта:

- политику доступа к сетевым сервисам;
- политику работы МЭ.

Политика доступа к сетевым сервисам определяет правила предоставления и использования всех возможных сервисов защищаемой компьютерной сети. В рамках данной политики должны быть заданы все сервисы, предоставляемые через МЭ, и допустимые адреса клиентов для каждого сервиса. Кроме того, для пользователей должны быть указаны правила, описывающие, когда, что, каким сервисом и на каком компьютере может воспользоваться. Задаются также ограничения на методы доступа, например на использования протоколов, SLIP (Serial Line Internet Protocol) и PPP (Point-to-Point Protocol). Ограничение методов доступа необходимо для того, чтобы пользователи не могли обращаться к «запрещенным» сервисам Internet обходными путями. Правила аутентификации пользователей и компьютеров, а также условия работы пользователей вне локальной сети организации должны быть определены отдельно.

Для того чтобы МЭ успешно защищал ресурсы организации, политика доступа пользователей к сетевым сервисам должна быть реалистичной. Реалистичной считается такая политика, при которой найден баланс между защитой сети организации от известных рисков и необходимым доступом пользователей к сетевым сервисам.

Политика работы МЭ задает базовый принцип управления межсетевым взаимодействием, положенный в основу функционирования МЭ. Может быть выбран один из двух принципов:

– запрещено все, что явно не разрешено;

– разрешено все, что явно не запрещено.

Фактически выбор принципа устанавливает, насколько «подозрительный» или «доверительной» должна быть система защиты. В

зависимости от выбора, решение может принято как в пользу безопасности и в ущерб удобству использования сетевых сервисов, так и наоборот.

В зависимости от типа экрана эти функции могут выполняться с различной полнотой. Простые МЭ ориентированы на выполнение только одной из них. Комплексные МЭ обеспечивают совместное выполнение указанных функций защиты. Собственная защищенность МЭ достигается с помощью тех же средств, что и защищенность универсальных систем. Чтобы эффективно обеспечивать безопасность сети, комплексный МЭ обязан управлять всем потоком, проходящим через него, и леживать свое состояние. Для принятия управляющих решений по используемым сервисам МЭ должен получать, запоминать, выбирать и обрабатывать информацию, полученную от всех коммуникационных уровней и от других приложений. Полнота и правильность управления требуют, чтобы комплексный МЭ имел возможность анализа и использования следующих элементов:

– информация о соединениях – информации от всех семи уровней в пакете;

– истории соединений – информации, полученной от предыдущих соединений;

– состояния уровня приложения – информации о состоянии, полученной из других приложений. Например, аутентифицированному до настоящего момента пользователю можно предоставить доступ через МЭ только для авторизованных видов сервиса;

– агрегирующих элементов – вычислений разнообразных выражений, основанных на всех вышеперечисленных факторах.

Основные схемы подключение МЭ. При подключении корпоративной сети к глобальным сетям необходимо разграничить доступ в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную сеть, а также обеспечить защиту подключаемой сети от удаленного НСД со стороны глобальной сети. При этом организация заинтересована в сокрытии информации о структуре своей сети и ее компонентов от пользователей

глобальной сети. Работа с удаленными пользователями требует установления жестких ограничений доступа к информационным ресурсам защищаемой сети. Часто возникает потребность иметь в составе корпоративной сети несколько сегментов с разными уровнями защищенности:

– свободно доступные сегменты (например, www-сервер);

– сегмент с ограниченным доступом (например, для доступа сотрудникам организации с удаленных узлов);

– закрытые сегменты (например, финансовая локальная подсеть организации).

Для подключения МЭ могут использоваться различные схемы, которые зависят от условий функционирования защищаемой сети, а также от количества сетевых интерфейсов и других характеристик, используемых МЭ. Широкое распространение получили схема:

– защиты сети с использованием экранирующего маршрутизатора;

– единой защиты локальной сети;

– с защищаемой закрытой и не защищаемой открытой подсетями;

– с раздельной защитой закрытой и открытой подсетей.

Если в составе локальной сети имеются общедоступные открытые серверы, то их целесообразно вынести как открытую подсеть до МЭ (рис.3.14).

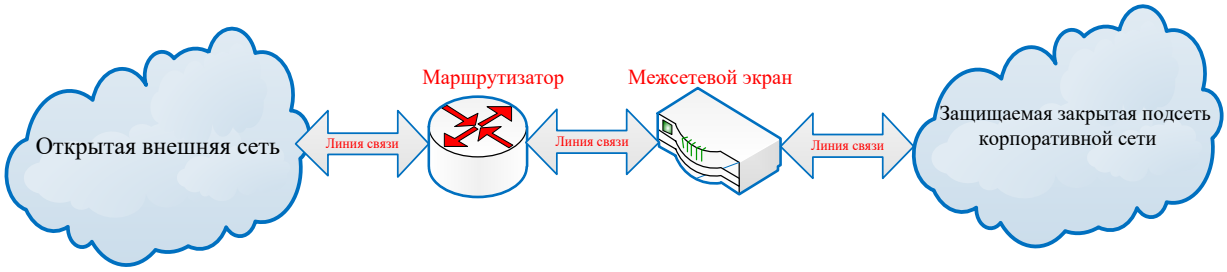

Рисунок 3.14 – Схема с защищаемой закрытой и не защищаемой открытой подсетями

Этот способ обладает высокой защищенностью закрытой части корпоративной сети, но обеспечивает пониженную безопасность открытых серверов, расположенных до МЭ.

Некоторые МЭ позволяют разместить эти серверы на себе. Однако такое решение не является лучшим с точки зрения безопасности самого МЭ и загрузки компьютера. Схему подключения МЭ с защищаемой закрытой подсетью и не защищаемой открытой подсетью целесообразно использовать лишь при невысоких требованиях по безопасности к открытой подсети. Если же к безопасности открытых серверов предъявляются повышенные требования, тогда необходимо использовать схему с раздельной защитой закрытой и открытой подсетей.

Персональные и распределенные сетевые экраны. За последние несколько лет в структуре корпоративных сетей произошли определенные изменения. Если раньше границы таких сетей можно было четко очертить, то сейчас это практически невозможно. Еще недавно такая граница проходила через все маршрутизаторы или иные сетевые устройства, через которые осуществлялся выход во внешние сети. В удаленных офисах банков ситуация была схожа. Однако сейчас полноправным пользователем защищаемой МЭ сети является сотрудник, находящийся за пределами защищаемого периметра. К таким сотрудникам банка относятся пользователи, работающие на дому или находящиеся в командировке. Несомненно, им также требуется защита. Но все традиционные МЭ построены так, что защищаемые пользователи и ресурсы должны находиться под их защитой с внутренней стороны корпоративной или локальной сети, что является невозможным для мобильных пользователей.

Для решения этой проблемы были предложены следующие подходы:

- применение распределенных МЭ (Distributed Firewall);
- использование возможностей виртуальных частных сетей VPN (Virtual Private Network);

Распределенный межсетевой экран (Distributed Firewall) – централизовано управляемая совокупность сетевых мини-экранов, защищающих отдельные компьютеры сети. Для индивидуальных пользователей представляет интерес технология персонального сетевого

экранирования. В этом случае сетевой экран устанавливается на защищаемый персональный компьютер. Такой экран, называемый персональным экраном компьютера (Personal Firewall) или системой сетевого экранирования, контролирует весь исходящий и входящий трафик независимо от всех прочих системных защитных средств. При экранировании отдельного компьютера поддерживается доступность сетевых сервисов, но уменьшается нагрузка, индуцированная внешней активностью. В результате снижается уязвимость внутренних сервисов защищаемого таким образом компьютера, поскольку первоначально сторонний злоумышленник должен преодолеть экран, где защитные средства сконфигурированы особенно тщательно и жестко. Эти средства не только защищают от внешних атак компьютеры, на которых они установлены, но и обеспечивают защиту трафика, передаваемого за пределы данного узла (т.е. организуют защищенные каналы VPN). Именно такое решение позволило обеспечить защиту сетей с нечетко очерченными границами. Наличие функции централизованного управления у распределенного МЭ – его главное отличие от персонального экрана. Если персональные сетевые экраны управляются только с компьютера, на котором они установлены, и идеально подходят для домашнего (или офисного) применения, то распределенные МЭ могут управляться централизованно, с единой консоли управления, установленной в главном офисе банка. Это позволило некоторым производителям выпускать МЭ в двух типах:

– персональной МЭ (для индивидуальных пользователей);

– распределенной МЭ (для корпоративных пользователей).

В современных условиях более 50% различных атак и попыток доступа к информации осуществляется изнутри корпоративных сетей, поэтому классический «периметровый» подход к созданию системы защиты корпоративной сети становится недостаточно эффективным. Корпоративную сеть можно считать действительно защищенной от НСД только при наличии в ней средств защиты точек входа со стороны Internet и решений,

обеспечивающих безопасность отдельных компьютеров, корпоративных серверов и фрагментов локальной сети предприятия. Решения на основе распределенных или персональных МЭ наилучшем образом обеспечивают безопасность отдельных компьютеров, корпоративных серверов и фрагментов локальной сети банков.

Использование возможностей виртуальных частных сетей VPN. Защита информации в процессе ее передачи по открытым каналам основана на использовании виртуальных защищенных сетей VPN (Virtual Private Network) называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных. Виртуальная защищенная сеть VPN формируется путем построения виртуальных защищенных каналов связи, создаваемых на базе открытых каналов связи общедоступной сети. Эти виртуальные защищенные каналы связи называются туннелями VPN. Сеть VPN позволяет с помощью туннелей VPN соединить головной офис, офисы филиалов, офисы бизнес-партнеров и удаленных пользователей и безопасно передавать информацию через Internet.

ЗАКЛЮЧЕНИЕ

Новые технологические возможности облегчают распространение информации, повышают эффективность бизнес процессов, способствуют расширению деловых отношений. Проблемы обеспечения информационной безопасности привлекают пристальное внимание как специалистов в области информационных технологий и сетей, так и многочисленных пользователей, включая компании, банковско-финансовые организации, работающие в сфере бизнеса. В этой связи, в первой главе монографии было проведено следующее:

– проанализированы кибератаки на банковские информационные системы, учтены международные и отечественные опыты;

– исследование основных видов кибератак;

– в настоящий момент в качестве одного из основных видов актуальных кибератак предложено считать DDoS-атаки.

Далее, по второй главе сделаны обобщения математических аппаратов для моделирования процессов кибератак на банковские информационные системы. Предложены частные модели для процессов кибератак на банковские информационные системы. Разработана методика оценки качества функционирования сетевых элементов БИС в условиях DDoS-атак злоумышленника. Разработана математическая модель процесса функционирования БИС на базе IP-технологии в условиях кибервоздействий.

Также, в третьей главе монографии, предложены методы защиты информации в банковских информационных системах, в частности:

– криптографические способы защиты информации в БИС;

– антивирусные программы и комплексы.

– основные методы повышения киберустойчивости корпоративной сети (БИС). Обосновано, что использование межсетевых экранов является весьма эффективным способом защиты корпоративной сети от DDoS-атак.

Дальнейшими направлениями развития положений, приведенных в данной монографии, являются:

– развитие методов динамического реконфигурирования и внедрения механизмов поддержания функциональной устойчивости системы;

– развитие интеллектуальных технологий анализа данных, машинного обучения для прогнозирования компьютерных атак;

– развитие методов раннего обнаружение вторжений с последующим реагированием объекта защиты на кибератаки и применения превентивных действий;

– разработка концепции функциональной устойчивости и кибербезопасности при проектировании и оценке безопасности цифровых банковских систем.

Применение различных моделей для разных классов цифровых систем позволит по-новому взглянуть на процессы развития их киберустойчивости в современных цифровых реалиях, предложить новые методы и средства защиты. Важно сказать, что киберустойчивость, как концепция, изменяет сам взгляд на безопасность, перенося фокус с параметров систем защиты и обрабатываемых данных, на характеристики защищаемого объекта. Формируется целевое представление о цифровой безопасности, а главным направлением будущих исследований уже сегодня стало выполнение целевой системой своих задач в условиях информационного противоборства.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативно-правовые документы и публикации методологического значения

1. Саммит ШОС в Астане 2017. Выступление президента РУзб. Ш.М. Мирзияева «О возникающих угрозах в глобальном информационном пространстве и противодействии им».

URL: http://ru.sputniknews uz.com/politics/20170609/ 5590266/Mirzieev

2. Закон Республики Узбекистан о Кибербезопасности.

URL: https://lex.uz/ru/docs/5960609

3. Официальный сайт Центрального Банка Республики Узбекистан.

URL: https://cbu.uz/ru/press_center/news/884303/

4. Официальный сайт Всемирного банка.

URL: https://www.worldbank.org/ru/access-to-information/overview

5. Официальный сайт «Лаборатории Касперского».

URL: https://www.kaspersky.ru

Диссертации, авторефераты, монографии и научные публикации

6. Бекбаев Г.А. Методика оценки функциональной целостности сети оперативно-корпоративной связи на участке высокоскоростной железнодорожной магистрали «Ташкент-Самарканд» АО «УТЙ»: дис. … канд. техн. наук: 05.12.13 / Г.А. Бекбаев. – СПб.: ПГУПС, 2018. – 155 с.

7. Евглевская Н.В. Методика комплексной оценки информационной безопасности телекоммуникационной сети единого дорожного диспетчерского центра управления перевозками ОАО «РЖД»: дис. … канд. техн. наук: 05.12.13 / Н.В. Евглевская. – СПб.: ПГУПС, 2016. – 164 с.

8. Скуднева Е.В. Методика маскирования информационного обмена в сетях передачи данных оперативно-технологического назначения ОАО

«РЖД»: дис. … канд. техн. наук: 05.12.13 / Е.В. Скуднева. – СПб.: ПГУПС, 2017. – 141 с.

9. Вандич А.П. Методика оценки оперативности управления телекоммуникационной сетью ОАО «РЖД» в нестандартных условиях: дис. … канд. техн. наук: 05.12.13 / А.П. Вандич. – СПб.: ПГУПС, 2013. – 142 с.

10. Бекбаев Г.А. Модель процесса «DDoS»-атаки на телекоммуникационную сеть железнодорожного транспорта / Г.А. Бекбаев, А.А. Привалов, Н.Б. Ачкасов, А.О. Кравцов // Изв. ПГУПС. – 2017. – Вып. 3 (52). – С. 420–426.

11. Бекбаев Г.А. “Моделирование процесса DDoS-атаки на банковские информационные системы”. Central Asian journal of mathematical theory and computer sciences. vol.3. Issue 10, 2022. p. 66-77.

12. Bekbaev G.A. “Information Security in the Financial and Banking System of the Republic of Uzbekistan”. Central Asian journal of mathematical theory and computer sciences. vol.3. Issue 02, 2022. p. 1-4.

13. Бекенова Я.А. Моделирование DDoS-атак и механизмов защиты от них / Я. А. Бекенова, Н.Н. Шипилов, К.А. Борисенко, А.В. Шоров // Изв. СПбГЭТУ «ЛЭТИ». 2015. – №3. – С. 32-39.

14. Н.И. Воропай, И.Н. Колосок, Е.С. Коркина, А.Б. Осак. Проблемы уязвимости и живучести киберфизических электроэнергетических систем // Энергетическая политика. Вып.5 . 2018 г., С. 53-62. - М. «Энергетическая политика», 2018. – 102 с.

15. Я. А. Бекенова. Анализ актуальных типов DDoS-атак и методов защиты от них. / Известия СПбГЭТУ «ЛЭТИ» № 1/2016. – С. 7-13.

16. Norros I. On the Use of Fractional Brownian Motion in the Theory of Connectionless Networks // IEEE Journal on Selected Areas in Communications.1995. Vol. 13. pp. 953-962.

17. Симонина О.А., Яновский Г.Г. Характеристики трафика в сетях IP // Труды учебных заведений связи./ СПБГУТ. СПб, 2004. № 171. С. 7-15.

18. Сепиашвили Д.М. Свойства трафика в сетях IP.// Труды учебных заведений связи./ СПБГУТ. СПб, 2004. № 176. С. 198-204.

19. Ложковский А.Г., Вербанов О.В. Моделирование трафика мультисервисных пакетных сетей с оценкой его коэффициента самоподобности// Научные труды ОНАС им. А.С. Попова. 2008. №1, С. 57-62.

20. Лосев Ю.И., Руккас К.М. Анализ моделей вероятности потери пакетов в буфере маршрутизатора с учетом фрактальности трафика // Вестник ХНУРЭ. Серия «Математическое моделирование. Информационные технологии. Автоматизированные системы управления. 2008. № 833. С. 163–169.

21. Одоевский С.М., Хоборова В.П. Методы прогнозирования качества обслуживания самоподобного трафика в усстройствах коммутации мультисервисной сети. // Труды учебных заведений связи. 2017. Т.3. № 3. С. 86-92.

22. Назаров А.Н., Сычев К.И. Модели и методы исследования процессов функционирования сетевых элементов сетей связи следующего поколения при произвольных распределениях поступления и обслуживания заявок различных классов качества. // Телекоммуникации и транспорт. №7, 2012г. С. 135-140.

23. Smirnov O., Didyk O., Dreyev O., Smirnov S. GERT model complex for cloud antivirus security of telecommunication system // Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 3, p. 251-262.

24. Смирнов А.А. Математическая GERT-модель технологии передачи метаданных в облачные антивирусные системы / В.В. Босько, А.А. Смирнов, И.А. Березюк, Мохамад Абу Таам Гани // Збірник наукових праць «Системи обробки інформації». – Випуск 1(117). – Х.: ХУПС – 2014. – С. 137-141.

25. Саенко И.Б., Лаута О.С., Котенко И.В. Применение метода преобразования стохастических сетей для моделирования мобильных

банковских атак.// Изв. вузов. Приборостроение. 2016. Т. 59, № 11. С. 928-933.

26. Доррер М.Г. Зырянов А.А. Оценка числовых характеристик GERT-сети на основе эквивалентных преобразований./ Образовательные ресурсы и технологии. 2014 г., Вып. 1 (4). С. 175-184.

Учебники, учебные пособия и другие литературы

27. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.

28. Ярочкин В.И. Информационная безопасность: учебник для студентов вузов. – М.: Гаудеамус, 2-е изд. – 544 с.

29. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.

30. Коцыняк М.А. Устойчивость информационно-телекоммуникационных сетей / М.А. Коцыняк, И.А. Кулешов, О.С. Лаута. – СПб.: Изд-во Политехн. ун-та, 2013. – 92 с.

31. Привалов А.А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ / А.А. Привалов; под.ред. В.П. Чемиренко. – СПб.: ВМА, 2000. – 166 с.

32. Диффи У. Первые десять лет криптографии с открытым ключом / ТИИЭР. Т. 76, 1988.- 245 с.

33. Касперский Е. Компьютерные вирусы: что это такое и как с ними бороться. М.: СК Пресс, 2008. 192 с.

34. Бойцев О.М. Защити свой компьютер на 100% от вирусов и хакеров / О.М. Бойцев. – СПб.: Питер, 2008. – 45 с.

35. Климентьев К. Е. Компьютерные вирусы и антивирусы: взгляд программиста. – М.: ДМК Пресс, 2013. – 656 с.

36. Бирюков А.А. Информационная безопасность, защита и нападение. – М.: ДМК Пресс, 2017. – 434 с.

37. Зайцев А.П. Технические средства и методы защиты информации: Учебник для вуза / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под общ. ред. А.П. Зайцева, А.А. Шелупанова. – М.: Машиностроение, 2009. – 508 с.

38. Конахович Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов. – Киев: МК-Пресс, 2005. – 288 с.

39. Корниенко А.А. Информационная безопасность и защита информации на железнодорожном транспорте: учеб.для вузов / А.А. Корниенко, М.А. Еремеев, В.Н. Кустов и др.; под. ред. А.А. Корниенко. – М.:УМЦ ЖДТ, 2014. – 448 с.

40. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2001.

41. Крылов В.В., Самохвалова С.С. Теория телетрафика и ее приложения. СПб.: БХВ–Петербург. 2005. 288 с.

42. Шелухин О.И., Тенякшев А.М., Осин А.В. Моделирование информационных систем./ Под ред. О.И. Шелухина.- М. «Радиотехника», 2005, .-368 с : ил.

43. Росляков А.В., Ваняшин С.В., Самсонов М.Ю., Шибаева И.В., Чечнева И.А. Сети следующего поколения NGN/ Под ред. Рослякова А.В. – М. Эко-Трендз, 2008, 424 с.

44. Кучерявый А.Е., Цуприков А.Л. Сети связи следующего поколения. – М. ФГУП ЦНИИС, 2006. – 278 с.

45. Назаров А.Н. Сычев К.И. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения. 2-е изд. Доп. И перераб. – Красноярск: Изд-во ООО «Поликом», 2011. – 491 с.

46. М.А. Коцыняк, И.А. Кулешов, А.М. Кудрявцев, О.С. Лаута Киберустойчивость информационно-телекоммуникационной сети/ – СПб.: Бостон-спектр, 2015. –150 с.

47. Golenko-Ginzburg D. Stochastic network models in innovative projecting. – Voronezh: Science Book Publishing House, 2011. – 356 p

48. Куделя В. Н., Привалов А. А. Методы математического моделирования систем и процессов связи. – СПб.: Изд-во Политехн. Ун-та, 2009. – 368 с.

49. Neumann K. Stochastic project networks: temporal analysis, scheduling and cost minimization. – Berlin: Springer-Verlag, 1990. – 238 p.

Интернет ресурсы и платформы

50. Анализ кибератак на банковско-финансовую систему

URL: https://www.tadviser.ru/index.php

51. Кибератаки на банковские сферы Южной Кореи.

URL: https://www.banki.ru/news/lenta/?id=10986490

52. Информационно-новостной портал Республики Узбекистан.

URL: https://www.uzreport.news/society/hakeri-sovershili-kiberataku-na-asakabank

53. Информационно-новостной портал Республики Узбекистан.

URL: https://nova24.uz/money/gruppa-mezhdunarodnyh-hakerov-atakovala-uzbekskij-bank

54. Информационно-новостной портал Республики Узбекистан.

URL: https://nova24.uz/incidents/v-tashkente-vzlomali-sistemu-davr-banka

55. Каждая шестая компания в России подверглась DDoS-атакам.

URL: https://blog.kaspersky.ru/2015-kazhdaya-shestaya-kompaniya-v-rossii-podverglas-ddos-atakam/15027

56. Анализ атаки DDoS. URL: http://bit.samag.ru/archive/article/1504