УДК 629.391

МЕТОДОЛОГИЯ ОЦЕНКИ ВЛИЯНИЯ КИБЕРАТАК НА БЕЗОПАСНОСТЬ ВИДЕОИНФОРМАЦИОННОГО РЕСУРСА В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

БАРАННИК В.В., ПОДЛЕСНЫЙ С.А., ШУЛЬГИН С.С.

Излагаются основные этапы методологии оценки влияния кибератак на безопасность видеоинформационного ресурса. Анализируются современные угрозы информационно-телекоммуникационных систем. Обосновывается актуальность защиты видеоинформационного ресурса. Описывается проявление наиболее существенных атак типа "Distributed Denial of Service". Предлагаются основные требования для технологии кодирования, которые обеспечивают требуемую защиту.

1. Введение

Стремительное развитие информационных технологий привело к широкому распространению передачи мультимедийных данных по информационно-телекоммуникационным сетям. Применение мультимедиа для передачи данных позволяет увеличить качество восприятия информации, так как человек уделяет наибольшее внимание визуальной информации. В настоящее время в интересах ведомственных организаций и профильных министерств передача мультимедийных файлов в одном направлении используется в системах видеомониторинга, а двунаправленная передача применяется в системах видеоконференцсвязи. На сегодняшний момент данные системы очень широко применяются в государственных ведомственных структурах для повышения качества управления по соответствующим направлениям деятельности. Как показывает практика в обычных условиях, особенно в кризисных ситуациях, повышаются угрозы применения злоумышленниками кибератак. В то же время вопросы, которые касаются исследований актуальности и значимости влияния различных кибератак на характеристики целостности и оперативности видеоинформационного ресурса в телекоммуникационной системе, недостаточно рассмотрены.

Поэтому необходимо разработать методологию, которая учитывает существующие механизмы функционирования телекоммуникационной системы и действия кибернетических атак на видеоинформационный ресурс.

Цель исследования состоит в том, чтобы предложить пути развития методов кодирования для обеспечения требуемой защиты информационной безопасности.

2. Описание процесса обработки видеопотока и доставки видеоинформационного ресурса в телекоммуникационной системе

Процесс обработки видеопотока и доставки данных в телекоммуникационной системе состоит из следующих основных этапов (рис. 1).

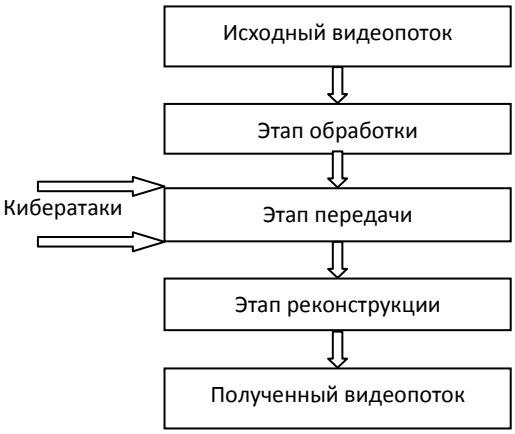

Рис. 1. Этапы обработки видеопотока

Рассмотрим каждый этап данного процесса.

1. *Этап обработки*. На данном этапе происходит подготовка изображения для его передачи в телекоммуникационной системе так, чтобы обеспечить необходимое качество на приемной стороне.

Оператор обработки функционирует на основе нескольких механизмов. В процессе сжатия видеоизображения используются следующие механизмы: устранение пространственной избыточности изображении, устранение временной избыточности видео, использование более низкого цветового разрешения при цветоразностном представлении изображения, повышение информационной плотности результирующего цифрового потока. Основными выходными параметрами на этапе обработки исходного видеопотока являются:

BR – битовая скорость кодированных данных;

Φ_K – время кодирования;

PSNR – отношение пикового уровня сигнала к шуму для изображения.

2. *Этап передачи*. На данном этапе производится передача видеопотока от источника к потребителю с применением телекоммуникационных технологий.

При использовании телекоммуникационных технологий учитываются следующие параметры: C – пропускная способность; P – вероятность потери бита при передаче данных.

Процесс функционирования информационно-телекоммуникационных систем определяется следующими операторами: $F_{AQM}(\lambda, \mu, W, S, QoS)$ – оператор обработки очередей пакетов; $F_{CRC}(P)$ – оператор проверки пакетов на ошибки при проверке пакетов; $F_{ROUTE}(Proto, AdrDst, PortDst, AdrSrc, PortSrc, TTL)$ – оператор маршрутизации пакетов.

Оператор обработки очередей пакетов функционирует на основе нескольких механизмов. В классическую схему системы управления трафиком входят следующие механизмы: ограничение исходящего трафика (shaping), планирование (scheduling), классификация (classifying), ограничение входящего трафика (policing), уничтожение (dropping), маркирование (marking) пакета. Данный оператор зависит от следующих характеристик:

λ – интенсивность входного потока;

μ – интенсивность обслуживания выходного потока;

W – емкость буфера коммутационного устройства;

S – размер пакета;

QoS – класс обслуживания.

Оператор маршрутизации пакетов функционирует на основании полученной информации об адресации сетевого уровня, которую он извлек из пакета данных. Этот оператор зависит от следующих характеристик:

Proto – наименование протокола;

AdrDst, PortDst – адрес и порт назначения;

AdrSrc, PortSrc – адрес и порт источника;

TTL – время жизни пакета.

3. *Этап реконструкции*. На данном этапе происходит декодирование информации и вывод изображения пользователю.

Оператор реконструкции функционирует на основе нескольких механизмов. В процессе реконструкции видеоизображения используются следующие механизмы: получение декодированного остаточного макроблока в процессе деквантования и обратного преобразования; получение восстановленного макроблока для отображении в декодированном кадре.

Для оценки качества воспроизведения видео при декодировании существенными являются следующие параметры:

$T_{ЗП}$ – задержка пакетов;

δ – джиттер пакетов;

$\nu_{пп}$ – количество потерянных пакетов.

Согласно рекомендациям международного союза электросвязи (МСЭ) [1] для системы видеосвязи задержка пакета не должна превышать $T_{ЗП} \le 150 мсек$, для видеопотока задержка пакета не должна превышать $T_{ЗП} \le 10 сек$, джитер пакетов не должен превышать $\delta \le 80 мсек$, количество потерянных пакетов не должно превышать $\nu_{ППП} \le 1\%$.

Эти параметры зависят от динамической характеристики среды передачи данных и операторов информационно-телекоммуникационных систем и даже при нормальных условиях (при отсутствии какого-либо вмешательства в работу системы извне) функционирования телекоммуникационных устройств возможны потери видеоинформационного ресурса. К примеру, вероятность потери бита информации при передаче в нормальных условиях в проводных системах составляет около 10^{-8}, а в беспроводных – около 10^{-3} [2].

Теперь рассмотрим, как изменятся параметры оценки качества воспроизведения видео в случае применения кибератак.

3. Влияние DDoS атак на информационно-телекоммуникационную систему

На информационно-телекоммуникационную систему могут воздействовать злоумышленники. Целью кибернетических атак злоумышленников является нарушение таких свойств информационной безопасности как целостность и доступность видеоинформационного ресурса.

В течение 2014 года специализированным структурным подразделением Государственного центра защиты информационно-телекоммуникационных систем (ГЦЗ ИТС) Государственной службы специальной связи и защиты информации Украины (Госспецсвязи) CERT-UA были приняты меры по реагированию на 216 компьютерных инцидентов [3]. Статистика по типам угроз и секторам возникновения приведена в табл. 1, 2. Данные приводятся в отношении тех инцидентов, по поводу которых CERT-UA было сообщено в установленном порядке.

Таблица 1

Соотношение угроз

Типы угроз	Количество	Доля %
DDoS	51	24
Несанкционированный доступ	39	18
Фишинг	30	14
Malware	25	12
Advanced Persistent Threat (APT)	25	12
Другое	46	21
Итого	216	100

Таблица 2

Распределение угроз по секторам

Типы угроз	Принадлежность сектора				
	UAGOV	UACOM	FGOV	FCOM	UACTZ
DDoS	43	2	3	3	0
Несанкционированный доступ	33	3	3	0	0
Фишинг	0	6	1	23	0
Malware	7	10	0	1	7
Advanced Persistent Threat (APT)	21	3	1	0	0
Бот-сети	5	6	2	2	1
Уязвимости	13	1	1	0	2
Мошенничество	2	6	0	0	0
Утечка информации	0	3	0	0	0
Другое	0	2	0	0	0
Итого	124	42	11	29	10

Как видно из указанных таблиц, наиболее распространенными видами кибератак (43 для украинского государственного сектора, 2 для украинского коммерческого сектора, 3 для зарубежного государственного

сектора, 3 для зарубежного коммерческого сектора) являются атаки типа DDoS-атака. Это связано, прежде всего, с легкостью реализации данного типа атаки.

При описании модели злоумышленника считается, что его тип будет профессионал или сотрудник предприятия. Для профессионала характерна способность добывать сведения об информационно-телекоммуникационной системе, планировать и готовить вторжение, у него имеется специальный набор средств для осуществления кибератак. Для сотрудника предприятия характерна способность добывать сведения об информационно-телекоммуникационной системе, планировать и готовить вторжение, произвести саботаж работы информационно-телекоммуникационной системы. У него имеется набор самодельных или доступных средств для осуществления кибератак ТСО, он действует скрытно в рабочее время.

В условиях применения атаки на телекоммуникационное устройство дополнительно действует оператор влияния атаки $F_A(\lambda_A, S_A, Proto_A)$.

Оператор влияния атаки на телекоммуникационное устройство функционирует на основании следующих характеристик:

λ_A – интенсивность атаки (количество пакетов),

S_A – размер пакета,

$Proto_A$ – наименование протокола.

На данный момент существует достаточно много различных видов атак на отказ, каждая из которых использует определенную особенность построения сети или уязвимости программного обеспечения.

Эти атаки могут осуществляться путем непосредственной пересылки большого количества пакетов (UDP, ICMP flood), использование атак на промежуточные узлы (Smurf, Fraggle), передачи слишком длинных пакетов (Ping of Death), некорректных пакетов (Land) или большого количества трудоемких запросов [4]. Заметим, что в последнее время происходит развитие этого направления деятельности и появление новых видов и способов атак. Из последних тенденций можно отметить появление атак ухудшения качества (Quality Reduction Attack) и низкочастотных атак (Low Rated Attack) Поэтому необходимы исследования и разработки новых методов противодействия.

Основные существующие классы атак достаточно хорошо изучены. Атаки классифицированы согласно протоколам, по которым они осуществляются. Выделены следующие атаки: SYN flood, TCP reset, ICMP flood, UDP flood, DNS request, CGI request, Mail bomb, ARP storm и атаки на алгоритмическую сложность.

Истощение ресурсов сети заключается в пересылке большого количества пакетов в сеть жертвы. Они уменьшают ее пропускную способность для законных пользователей. Существует несколько видов таких атак:

UDP/ICMP flood заключается в пересылке значительного количества крупных (фрагментированных) пакетов по протоколам UDP/ICMP;

Smurf/Fraggle заключается в пересылке пакетов UDP/ICMP ECHO на широкий диапазон адресов со сфальсифицированого IP адреса. При этом на адрес жертвы приходит большое количество пакетов-ответов.

Истощение ресурсов узла заключается в пересылке трудоемких или некорректных запросов жертве. К этому виду относятся следующие атаки:

TCP SYN – сознательное прерывание процесса установления соединения и создание большого количества полуоткрытых TCP/IP соединений (поскольку это число ограничено, то узел перестает принимать запросы на соединение);

Land – пересылка пакета TCP SYN с одинаковыми адресами получателя и источника и портами (при посылке таких пакетов узел с Windows NT зависает);

Ping of Death – посылка пакета “ping” очень большой длины, который ОС не может обработать;

пересылка некорректных пакетов, при обработке которых на узле могут возникнуть ошибки;

пересылка трудоемких запросов для загрузки узла.

Достаточно эффективной формой отраженной атаки является использование серверов доменных имен (Domain Name System (DNS) servers). Схематически данная атака показана на рис. 2.

Эти серверы нужны для хранения и предоставления по требованию различных записей (Resource records (RR)) с именами доменов Интернет. В такой записи могут быть данные типа TXT RR, в которые администратор может внести произвольный текст, типа A RR, где определяется отображение имени в 32-битную IP адрес, и типа SOA1 RR, где определяется имя домена Интернет и другая сопутствующая информация. Важнейшей функцией DNS серверов является трансляция доменных имен в IP адреса. После получения запроса на IP адрес DNS сервер пытается найти соответствующую запись в своей базе данных. Если это не удалось, то запрос рассылается по всем известным ему DNS серверам. Эта процедура называется рекурсивным запросом. Размеры запроса и ответа могут существенно отличаться. Обычно ответ содержит первоначальный запрос и ответ. Это означает, что ответ всегда больше запроса. Более того, ответ может содержать различные типы RR данных и некоторые из них могут иметь значительный объем. Теоретически, начальный трафик мощностью 140 Mb/s с ботнет может привести к потоку DNS ответов мощностью 10 Gb/s.

Как видно из указанного, при существующей модели обработки и доставки видеоинформационного ресурса телекоммукационное устройство будет обрабатывать большой поток информации. При существующих механизмах его работы происходит задержка переда-

чи пакетов с возможным их отбрасыванием. Основной результат DDoS-атаки на телекоммуникационное устройство заключается в изменении времени прохождения и общего количества пакетов информации для видеоинформационного ресурса.

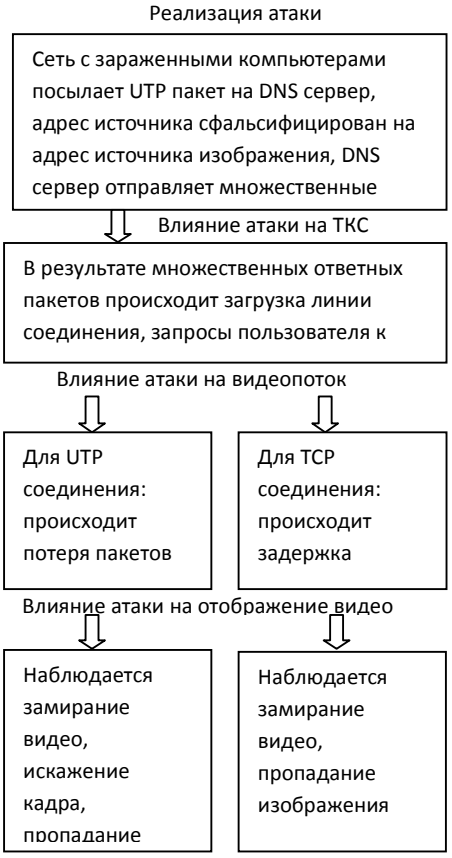

Рис. 2. Влияние атаки типа "DNS Amplification Attacks" на передачу видеоинформационного ресурса в информационно-телекоммуникационной системе

Для предупреждения возникновения атаки типа DDoS-атака могут применяться системы обнаружения и предотвращения вторжений, управляемые коммутаторы со списками контроля доступа и резервирования линий связи между отдельными узлами [5].

К недостаткам перечисленных методов относятся вносимые через обработку пакетов задержки, и как результат ограничение скорости передачи сигнала в сети, увеличенная стоимость оборудования и подписки на сигнатуры, данными методами не обеспечивается защита от замаскированных вирусных атак.

Поэтому необходимо разработать новый метод прогнозирования и локализации атак, который учитывает этап кодирования источника и обеспечивает требуемую степень соответствия полученной информации показателям класса обслуживания в условиях применения DDoS-атак, когда возможны задержки передачи пакетов с возможным их отбрасыванием.

4. Выводы

1. Разработана методология оценки влияния кибератак на безопасность видеоинформационного ресурса в телекоммуникационной системе.

Эта методология основана на описании процесса обработки и доставки данных, учитывает существующие операторы и механизмы процесса. Она призывает разработать новый метод прогнозирования и локализации атак, который учитывает этап кодирования источника и обеспечивает требуемую степень соответствия полученной информации показателям класса обслуживания.

2. Обосновано, что DDoS-атаки влияют на передачу в информационно-телекоммуникационной системе. Это приводит к потере целостности и доступности видеоинформационного ресурса.

3. Показано, что существующие технологии противодействия DDoS-атак не обеспечивают в полной мере их локализацию и предупреждение (т.е. они работают с последействием, запаздыванием, после распознания факта применения атаки). Также немаловажен тот факт, что в случае выявления кибератаки существующие системы противодействия DDoS-атак отсекают входящий поток данных, из-за чего происходит потеря "полезной" информации, т.е. ухудшаются такие характеристики безопасности видеоинформационного ресурса, как целостность и доступность.

Литература: 1. *Рекомендации* Международного союза электросвязи ITU-T G.1010 "End-User multimedia QoS categories". **2**. *Олифер В.Г.* Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов / В.Г. Олифер, Н.А. Олифер. СПб.: Питер, 2006. 958 с. **3.** *Звіт* CERT-UA за 2014 рік, http://cert.gov.ua/?p=2019, 2015. **4**. Peng Liu. Denial of Service Attacks – University Park. 2004. **5**. *Мартынюк И.* Материалы технического тренинга «Построение безопасных сетей на оборудовании D-Link», http://service.d-link.ua/sites/default/files/files/Security.zip, Киев, 2012. 190с.

Поступила в редколлегию 21.02.2016

Рецензент: д-р техн. наук, проф. Безрук В.М.

Баранник Владимир Викторович, д-р техн. наук, профессор, начальник кафедры Харьковского университета Воздушных Сил. Научные интересы: кодирование и защита информации для передачи в телекоммуникационных системах. Адрес: Украина, 61000, Харьков, ул. Сумская, 77/79. E-mail: barannik_v_v@mail.ru.

Подлесный Сергей Анатолиевич, начальник отделения Харьковского университета Воздушных Сил. Научные интересы: кодирование и защита информации для передачи в телекоммуникационных системах. Адрес: Украина, 61000, Харьков, ул. Сумская, 77/79. E-mail: serg380638472732@gmail.com

Шульгин Сергей Сергеевич, соискатель Национального авиационного университета. Научные интересы: кодирования, семантической обработки изображений. Адрес: Украина, Киев, пр. Космонавта Комарова, 1.