УДК 004.056

О.С. Макарова

Методика формирования требований по обеспечению информационной безопасности сети IP-телефонии от угроз среднестатистического «хакера»

Предложен подход к формированию требований по обеспечению информационной безопасности корпоративной сети IP-телефонии. Рассмотрены результаты применения данного подхода для одного типа нарушителей – среднестатистический «хакер». Определен подход к дифференциации требований в зависимости от изменения ценности активов организации.
Ключевые слова: сеть IP-телефонии, требования по обеспечению информационной безопасности, среднестатистический «хакер».

Актуальность задачи

Отсутствие требований по обеспечению информационной безопасности корпоративных сетей IP-телефонии является актуальной проблемой.

В настоящее время в крупных организациях осуществляется планомерный переход к сетям IP-телефонии [1]. Это обусловлено экономической эффективностью использования сетей IP-телефонии, оценка которой проведена в работе [2], ростом числа комплексных решений по построению унифицированных коммуникаций, реализующих технологию IP-телефонии, по данным аналитических исследований Gartner, Inc [3], решением вопроса, связанного с повышением эффективности передачи речевой информации, улучшением качества связи в корпоративных IP-сетях в рамках проводимых научных исследований [4–6].

В то же время конвергенция информационных и телекоммуникационных технологий приводит к появлению новых угроз информационной безопасности, специфичных только для технологии IP-телефонии. В настоящее время в рамках существующей нормативной базы обеспечения информационной безопасности сетей электросвязи, разделы 6–8 ГОСТ Р 52448–2005 [7], определены только направления формирования требований по обеспечению информационной безопасности. Таким образом, на данный момент отсутствуют нормативные документы, определяющие требования по обеспечению информационной безопасности сети IP-телефонии. В соответствии с Федеральным законом «О связи» [8] ответственность в выборе необходимых и достаточных мер и средств защиты средств и линий связи лежит на организации.

Анализ международных стандартов и рекомендаций («best practice») [9, 10] показывает, что сформированные в данных документах перечни угроз информационной безопасности сетей IP-телефонии и требования по защите от данных угроз не являются полными. В международном стандарте NIST [9] не отражены такие типы угроз, как «вишинг» (получение конфиденциальной информации путем обмана) и SPIT (передача нежелательной информации с использованием IP-телефонии), и способы защиты от них. Международные рекомендации VOIPSA [10] не содержат угрозы, связанные с объективными факторами воздействия (природные катаклизмы), недостатками в проектировании сети IP-телефонии. Кроме того, в рамках данных стандартов описание сценариев реализации угроз приведено лишь частично, сформулированные требования не дифференцированы, например, в зависимости от типа оконечного устройства (программный или аппаратный IP-телефон). Требования и решения по обеспечению информационной безопасности сети IP-телефонии, описанные в данных документах [9, 10], не учитывают особенности законодательства Российской Федерации по обеспечению информационной безопасности [11–13], соответственно не могут в полной мере применяться в Российской Федерации. Отсутствие сформулированных требований по обеспечению информационной безопасности сети IP-телефонии может привести к использованию неоправданно дорогостоящих решений при построении системы защиты или наличию уязвимостей в ней.

Подход к решению задачи

Перечень требований по обеспечению информационной безопасности сети IP-телефонии в Российской Федерации может быть сформирован путем выделения типовых сценариев реализации

угроз. Формирование типовых сценариев реализации угроз позволит сгруппировать возможные атаки на сеть IP-телефонии, выявить эксплуатируемые во время атаки уязвимости и определить необходимые и достаточные требования по защите. Сценарии реализации угроз в первую очередь определяются источником угроз информационной безопасности, в частности, – моделью нарушителя. Классификация нарушителей, предлагаемая в рамках данной работы, проводится в зависимости от возможностей нарушителя.

Одним из типов выделяемых нарушителей является среднестатистический «хакер». Анализ исследований [14, 15] показывает, что среднестатистический «хакер» для реализации атаки использует методы, описание которых представлено в сетях связи общего пользования, бесплатное или свободно распространяемое программное обеспечение. К этому типу можно отнести злоумышленников, осуществляющих свою деятельность из сетей связи общего пользования или сети передачи данных организации. Мотивы, которыми руководствуются нарушители данного типа, – денежная выгода и самоутверждение. Неформальная модель среднестатистического «хакера» позволяет сделать вывод, что сценарии реализации угроз, характерные для данного типа нарушителя, можно сформировать, проводя анализ описаний атак в сетях связи общего пользования.

Поиск вариантов реализации атак проводился через наиболее популярные в России поисковые системы, по результатам исследований comScore, Inc и Dilibrium, Inc [16,17]: Яндекс, Google, Mail.ru. При сборе данных использовались русско- и англоязычные запросы (количество слов в запросе варьировалось от 3 до 5), анализировались первые десять результатов поиска, а также ссылки, полученные при анализе содержимого страниц, найденных по запросу. Для получения полной картины возможных атак были сформированы основные категории угроз для данного типа нарушителей, путем анализа ГОСТ Р 52448–2005 [7], международных стандартов и рекомендаций:

– перехват трафика;
– модификация трафика;
– отказ в обслуживании;
– несанкционированный доступ к средствам связи;
– мошенничество;
– социальная инженерия.

При сборе данных формировалось одинаковое количество запросов (10) по каждому классу угроз.

Полученные результаты

Используя описанный в предыдущем разделе подход, была собрана статистика атак на сеть IP-телефонии – было проанализировано около 600 web-страниц с описанием алгоритмов и средств, используемых при реализации атак. Все атаки были разбиты на базовые, т.е. атаки, приводящие к реализации одной из сформированных выше категорий угроз. Процентное соотношение базовых атак, которые может осуществить среднестатистический «хакер», для каждой категории угроз приведено на рис. 1. Ниже даны характеристика полноты и точности полученных результатов – обоснована необходимость анализа именно первых десяти результатов поиска и ограничения, накладываемые количеством сформированных запросов.

Поисковые системы при формировании результатов поиска опираются на частоту появления слов запроса в тексте web-страницы. В соответствии с данными исследований [18] частота появления слов запроса в тексте web-страницы, достаточная для попадания web-страницы в первые десять результатов запроса, составляет в среднем 6 процентов. Используя закон Ципфа, получаем, что для одиннадцатой web-страницы частота появления слова из нашего запроса составляет 0,54%. Корректность использования закона Ципфа для электронных ресурсов обоснована в исследовательской работе [21]. Среднее число слов на странице [19] составляет 478. Таким образом, количество слов из нашего запроса на одиннадцатой web-странице составляет примерно 2. В соответствии с данными исследований [20] оптимальное количество ключевых слов в запросе должно быть 3–5, соответственно при количестве слов в запросе больше 2, нецелесообразно анализировать результаты поиска дальше десятой web-страницы.

В соответствии с [15] среднестатистический «хакер» рассчитывает на быстрое достижение результата, соответственно на поиск сценария реализации атаки он не потратит много времени. Чтение одной web-страницы в среднем составляет 10 мин, соответственно на анализ результатов 10 запросов по интересующему нарушителя направлению реализации атаки будет потрачено около 16 ч, вероятнее всего, что если данный тип нарушителя не подберет за это время сценарий реализации

атаки, то переключится на реализацию другой задачи. Таким образом, сформированной выборки достаточно для проведения анализа сценариев реализации атак среднестатистического «хакера».

Рассмотрим более подробно полученные результаты, представленные на диаграмме (см. рис. 1). Наибольшее количество описанных в сетях связи общего пользования методов реализации атак (35%) приводит к реализации угрозы отказа в обслуживании средств связи. Необходимо отметить, что угрозы данного класса (30% случаев) являются следствием реализации угрозы перехвата трафика (сигнализации, речевой информации, управляющей информации). Хотелось бы отдельно отметить категорию угроз – социальная инженерия. Данная категория в большей степени зависит от психологических особеннос-тей нарушителя и абонента, соответственно, в дальнейшем будет рассмотрена отдельно.

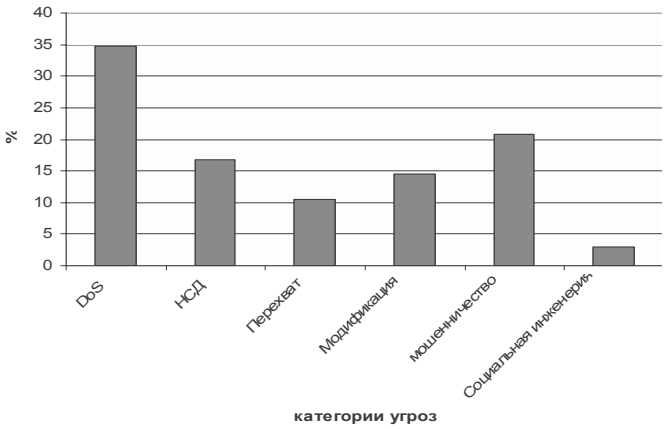

Рис. 1. Процентное соотношение количества типов атак, относящихся к каждой категории угроз

Анализируя полученные данные, выделим типовые сценарии реализации угроз на отказ в обслуживании: общие – сценарии реализации угроз на отказ в обслуживании, не учитывающие специфику технологии IP-телефонии, и специализированные, учитывающие особенности технологии IP-телефонии.

К общим типам сценариев реализации угроз относятся:

– атаки, приводящие к отказу в обслуживании сети передачи данных;

– атаки, приводящие к отказу в обслуживании операционной системы или базовой системы ввода-вывода средств связи.

К специализированным типам сценариев реализации угроз относятся:

– атаки, приводящие к отказу в обслуживании, использующие уязвимости реализации программного обеспечения средств связи;

– атаки, приводящие к отказу в обслуживании, реализуемые путем отправки большого количества запросов неверного формата для прохождения авторизации;

– атаки, приводящие к отказу в обслуживании, реализуемые путем отправки большого количества корректных запросов для прохождения авторизации с неверными учетными данными;

– атаки, приводящие к отказу в обслуживании с использованием специальных запросов, приводящих к аварийному завершению работы средств связи;

– атаки, приводящие к отказу в обслуживании путем переполнения буфера обмена и памяти пакетами корректного формата (используя протоколы TCP, SIP, H.323, RTP);

– атаки, приводящие к отказу в обслуживании путем переполнения буфера обмена и памяти пакета некорректного формата (некорректное значение полей, нестандартный объем пакета);

– косвенные атаки, приводящие к отказу в обслуживании средств связи, на которые настроено перенаправление вызовов (пакетов), например сервер голосовой почты;

– атаки, приводящие к отказу в обслуживании путем отправка сообщений, отменяющих и завершающих соединение на оконечные устройства при попытке установить соединение между ними;

– атаки, приводящие к отказу в обслуживании путем отправки сообщений о том, что абонент занят или отсутствует, что приводит к невозможности получения вызовов абонентом;

– атаки типа «человек посередине», приводящие к отказу в обслуживании, нарушитель может разорвать соединение.

Детальный анализ сценариев реализации угроз позволяет сформировать перечень требований по их устранению.

В общем случае перечень мер защиты включает как мероприятия по предотвращению и обнаружению атак, так и мероприятия по оперативному устранению последствий атак.

Мероприятия по предотвращению атак могут включать в себя:

– корректную настройку средств связи (отключение не используемых сервисов, портов);

– периодическое обновление программного обеспечения;

– наличие высококвалифицированных специалистов;

– использование средств предотвращения вторжений на уровне оконечного устройства;

– использование средств предотвращения вторжений и средств межсетевого экранирования на уровне сети передачи данных, специализированных на технологии IP-телефонии;

– аутентификацию средств связи и абонентов в сети IP-телефонии;

– использование систем имитации сети IP-телефонии или средств связи («honeypot»).

Мероприятия по обнаружению атак могут включать в себя:

– использование средств обнаружения вторжений на уровне оконечного устройства;

– использование средств обнаружения вторжений на уровне сети передачи данных, специализированных на технологии IP-телефонии;

– ведение подробного журнала регистрации событий (не только стандартная информация о начале и окончании соединения);

– периодический анализ журналов регистрации событий.

Мероприятия по устранению последствий атак могут включать в себя:

– резервирование средств и линий связи;

– наличие плана восстановления сети IP-телефонии.

Реализация большинства из этих мероприятий может осуществляться как организационными мерами, так и техническими, соответственно стоимость и результативность системы защиты могут быть различными. Поэтому следующая задача – проведение дифференциации и конкретизации требований. Конкретизация требований будет проведена на основе детального анализа типовых сценариев реализации угроз, которые в рамках данной статьи лишь обозначены. Дифференциация требований будет проводиться, используя мягкую модель Мальтуса, модель сражения Ланкастера и теорию вероятности, при расчете изменения ценности актива организации при внедрении мер защиты и реализации сценария реализации угроз, при расчете достаточности мер защиты для поддержания необходимой ценности актива.

Заключение

Обоснована актуальность и необходимость формирования требований по обеспечению информационной безопасности сети IP-телефонии, определен подход к формированию и градации требований, в том числе математический аппарат, который используется в рамках данного подхода.

Предложен метод классификации нарушителей информационной безопасности сети IP-телефонии, приведено неформальное описание одного из типов нарушителей – среднестатистического «хакера». Описаны подход к формированию типовых сценариев угроз, которые может осуществить среднестатистический «хакер», а также результаты, полученные при применении данного подхода.

В дальнейших публикациях планируется провести описание других типов нарушителей, типовых сценариев угроз, которые они могут реализовать; описание уровней требований по обеспечению информационной безопасности сети IP-телефонии и возможные методы выполнения требований.

Литература

1. Надежное партнерство [Электронный ресурс]. – Режим доступа: http://www.nateks.ru/pub/index.php?lpub=97&link=pub, свободный (дата обращения: 02.04.2012).

2. Петров А.А. Методы определения эффективности применения технологии IP-телефонии в информационных структурах железнодорожного транспорта: дис. … канд. техн. наук. – М., 2006. – 193 с.

3. Gartner Magic Quadrant for Unified Communications 2011 [Электронный ресурс]. – Режим доступа: http://msunified.net/2011/08/25/gartner-magic-quadrant-for-unified-communications-2011/, свободный (дата обращения: 02.04.2012).

4. Костенко А.И. Алгоритм повышения качества речи в сетях с пакетной коммутацией замещением потерянных пакетов на основе квазипериодической структуры речи: дис. … канд. техн. наук. – М., 2010. – 165 с.

5. Юрченко Д.Ю. Методы повышения эффективности применения технологий широкополосного доступа на железнодорожном транспорте: Дис. … канд. техн. наук. – М., 2007. – 186 с.

6. Сычев К.И. Модели и методы исследования процессов функционирования и оптимизации построения сетей связи следующего поколения (Next Generation Network): дис. … канд. техн. наук. – М., 2009. – 385 с.

7. ГОСТ Р 52448–2005 Национальный стандарт Российской Федерации. Защита информации. Обеспечение безопасности сетей электросвязи общие положения. – Введ. 01.01.2007. – М.: Стандартинформ, 2006. – 13 с.

8. Российская Федерация. Законы. Федеральный закон о связи №126 // Рос. газ. – 2003. – 25 июня.

9. D. Richard Kuhn, Thomas J. Walsh, Steffen Fries. Recommendations of the National Institute of Standards and Technology / D. Richard Kuhn, Thomas J. Walsh, Steffen Fries; Security considerations for voice over IP systems. – NIST Special Publication 800-58 – 01.01.2005. – P. 99.

10. VOIPSA. VoIP Security and Privacy Threat Taxonomy. – VOISPA. – 24.10.2005. – 36 с.

11. Российская Федерация. Законы. Федеральный закон об электронной подписи № 63 // Рос. газ. – 2011. – 06 апр.

12. ГОСТ 28147-89 Национальный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – Введ. 01.07.1990. – М.: ИПК Изд-во стандартов, 1989. – 25 с.

13. ГОСТ 34.11-94 Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хеширования. – Введ. 23.05.1994. – М.: Госстандарт России, 1994. – 16 с.

14. Хакер и хакерша: первая научная типология [Электронный ресурс]. – Режим доступа: http://www.dw.de/dw/article/0,,921281,00.html, свободный (дата обращения: 16.04.2012).

15. Who is the typical Russian hacker? [Электронный ресурс]. – Режим доступа: http://www.net-security.org/secworld.php?id=9739, свободный (дата обращения: 16.04.2012).

16. Рейтинг поисковых систем за 2011–2012 год от компании Dilibrium [Электронный ресурс]. – Режим доступа: http://mir.dilibrium.ru/stati/43-stati-o-internet-reklame/381-rejting-poiskovyh-sistem-za-2011-2012-god-ot-kompanii-dilibrium, свободный (дата обращения: 16.04.2012).

17. Russia Has Most Engaged Social Networking Audience Worldwide [Электронный ресурс]. – Режим доступа: http://www.comscore.com/Press_Events/Press_Releases/2010/10/Russia_Has_Most_Engaged_Social_Networking_Audience_Worldwide, свободный (дата обращения: 16.04.2012).

18. Как определить оптимальную частоту употребления ключевого слова (из поискового запроса, по которому продвигается статья) [Электронный ресурс]. – Режим доступа: http://ktonanovenkogo.ru/seo/search/poiskovaya-optimizaciya-sajta-seo-ranzhirovaniye-klyuchevye-slova-dlina-teksta-top-poiskovoj-vydachi.html, свободный (дата обращения: 16.04.2012).

19. Average Web Page Characteristics [Электронный ресурс]. – Режим доступа: http://www.websiteoptimization.com/speed/tweak/average-web-page/, свободный (дата обращения: 16.04.2012).

20. Оптимальный поисковый запрос должен содержать 3-5 слов [Электронный ресурс]. – Режим доступа: http://www.seo-altweb.ru/news/2010.08.08_zapros/, свободный (дата обращения: 16.04.2012).

21. Писляков В.В. Информетрическое моделирование процесса обращения к электронным информационным ресурсам: дис. … канд. техн. наук. – М., 2008. – 155 с.

Макарова Ольга Сергеевна
Аспирантка каф. теоретических основ радиотехники Уральского федерального университета
Тел.: 8-912-629-18-58
Эл. почта: osmakarova@list.ru

Makarova O.S.

Approach of formation of requirements for IP-telephony information security from threats of average «hacker»

Approach of formation of requirements for corporate IP-telephony information security is offered. Results of using this approach for one type of attacker – average «hacker» are considered. The approach to differentiate requirements depending on change of value of assets of the organization is defined.

Keywords: IP-telephony, requirements for IP-telephony information security, average «hacker».